Certificate Issuing and Management Components

Protection Profile

NIST PKI Project Team

September 30, 2000

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

This section includes an overview of the CIMC Protection Profile.

1.1 Identification

Title: Certificate Issuing and Management Components (CIMCs) Protection Profile

Registration: TBD

ISO/IEC 15408 version: 2.1

Keywords: Public Key Infrastructure, PKI, Certificate Issuing and Management Component, CIMC

1.2 Overview

A Public Key Infrastructure (PKI) is an architecture that is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings and provide other services critical to managing public keys. A PKI consists of many components. A Certificate Issuing and Management System (CIMS) includes the components of the PKI that are responsible for the issuance, revocation, and overall management of certificates and certificate status information. A CIMS always includes a Certification Authority (CA) and may include Registration Authorities (RAs) and other subcomponents.

A Certificate Issuing and Management Component (CIMC) consists of the hardware, software, and firmware that are responsible for performing the functions of a CIMS. A CIMC does not include environmental controls (e.g., controlled access facility, temperature), policies and procedures, personnel controls (e.g., background checks and security clearances), and other administrative controls.

This Protection Profile (PP) specifies the functional and assurance security requirements for a CIMC. The intent of this document is to ensure specification of the complete set of requirements for a CIMC and not the specification of a subset of requirements implemented in a specific CIMC subcomponent. It includes all the technical features of a CIMC, regardless of which CIMC subcomponent performs the function. The document does not differentiate between functions that are typically performed by a CA and functions that are typically performed by a RA.

Identifying all the subcomponents of a CIMC as a single entity assists in ensuring that the subcomponents compliant with the security requirements in this document will operate in a secure manner. This approach also ensures compatibility because a single vendor (or integrator) typically develops (or bundles) all the subcomponents together as a single solution. Typically, this is consistent with the way products are currently designed and built. A single product solution may make purchasing decisions easier because the user (or procurer) will not need to select subcomponents that meet a subset of the requirements. Finally, a single solution approach promotes security because the CIMC must:

- Implement all the mandatory security requirements, regardless of how they are allocated to subcomponents, and
- Ensure that functions implemented in one subcomponent do not compromise the security functions implemented in other subcomponents.

1.2.1 CIMC Keys

It is essential that private and secret keys in CIMCs be managed securely. For the purposes of this document, keys are separated into three categories based on the individual or device that is authorized to use the key:

1. *CIMS personnel keys*: Private and secret keys used within a CIMC designated for use by individual identities. CIMS personnel keys may be used for authentication, to sign information contained within or output by a CIMC, or to encrypt information files.

2. *Component keys*: Keys, other than CIMS personnel keys, which are used by the CIMC. CIMCs shall use Component keys to sign certificates and certificate status information. Component public/private key pairs may also be used in key agreements, for signing audit logs and system backups and for ensuring the integrity of transmitted or stored data. Component secret keys may be used to encrypt CIMC stored or transmitted data and compute authentication codes.
3. *Certificate subject private keys*: Private keys corresponding to the public keys contained in certificates issued by the CIMC where:
   - the private key is held by the CIMC solely to enable key recovery; or
   - the CIMC generates a public/private key pair and the private key is only held by the CIMC until the certificate subject has received it.

1.2.1.1 Cryptographic Functions Involving Private or Secret Keys

Private and secret keys within a CIMC are separated into different usage categories as described below. Listed in brackets next to each usage category are the associated key user categories defined in the CIMC Keys section.

1. *Certificate and Status Signing Keys*: Private keys used to sign certificates, CRLs, or other statements about the status of certificates. [Component keys]
2. *Integrity or Approval Authentication Keys*: Private or secret keys used to protect the integrity of transactions between CIMCs or CIMC subcomponents. Private or secret keys used to authenticate transactions between CIMCs that cause or approve the issuance or revocation of certificates. [CIMS personnel keys, Component keys]
3. *General Authentication Keys*: Private or secret keys used to authenticate users, messages, or sessions that do not include the authorization or approval of certificate issuance or revocation, but may include requests to issue or revoke certificates. [CIMS personnel keys, Component keys]
4. *Long Term Private Key Protection Keys*: Secret or private keys that are used to protect private keying material that is used for multiple sessions or messages. [CIMS personnel keys, Component keys]
5. *Long Term Confidentiality Keys*: Secret keys that are used to protect the confidentiality of security-relevant information such as PINS or passwords. This information does not include private keying material. [CIMS personnel keys, Component keys]
6. *Short Term Private Key Protection Keys*: Private keys used to protect keying material for a single session or message. [CIMS personnel keys, Component keys]
7. *Short Term Confidentiality Keys*: Secret keys used to protect a single session or message that does not contain keying material. [CIMS personnel keys, Component keys]

1.2.2 Data Input

A CIMC may receive information in many different ways. Data input is organized in the following three categories depending on the source of the data (local or remote) and whether the user is authenticated by the CIMC.

1. *Unauthenticated Data Entry:* The message/data may either be entered locally or received over a network. The originator of the message/data cannot be verified i.e., the user is unauthenticated.
2. *Local Data Entry:* A user, operating locally, enters or accepts data so that the CIMC can associate the data with the user and list the user in the audit log with the accepted data. The data entry could take the form of a user vouching for information that has already been entered into the computer by clicking on an “accept” button or by otherwise indicating acceptance of the information.

3. *Remote Data Entry:* The data could be received over a network in such a way that it can be bound to the identity of the sender of the data (or to the identity of some other remote user). For example, the data could be sent in a signed email.

1.2.3 Trusted Public Key Entry, Deletion, and Storage

In addition to issuing public key certificates, CIMCs may use public keys for their own purposes. Specifically, a CIMC may use the public key of another entity to encrypt messages that it intends to send to that entity, authenticate messages that it receives from that entity, or perform a key agreement to establish a session key for communicating with that entity.

A public key may be trusted by a CIMC because it is contained in a certificate that was issued by a CA that the CIMC trusts. At the next level, trust in the public key used to verify the signature on that certificate must be established. Trust in this public key may be established by another certificate. This trust validation *path* will continue until the final (or root) public key is reached. In order to bootstrap the process at the root public key, a CIMC must establish trust in this public key through some means other than certificate path processing. While the signatures on public key certificates authenticate and protect most public keys, a digital signature does not protect these public key "trust anchors". Also, these public keys must be protected from modification.

Every CIMC that uses public keys for authentication, encryption, integrity, or access control will maintain a list of trusted public keys. This list may include several keys (e.g., one for each authorized user) or may include only one key, which can be used to verify trust in all other public keys through path validation.

1.2.4 CIMC Security Levels

CIMCs will be operated in a wide variety of environments, from a closed secure facility to an open access facility in a hostile environment. Also, the sensitivity of the information protected by the certificates issued by CIMCs will vary significantly. Users will be required to evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity of the information. To address the varying levels of risk, this document specifies security requirements at four increasing, qualitative levels of security: Security Level 1, Security Level 2, Security Level 3, and Security Level 4.

1.2.4.1 **Security Level 1**

Security Level 1 provides the lowest level of security. CIMCs designed to meet the security requirements at Security Level 1 may be appropriate for use in environments in which the threat of malicious activity is considered to be low. CIMCs at Security Level 1 do not provide protection against unauthorized disclosure by malicious authorized or unauthorized users. At this Level, the CIMC provides functions appropriate to a PKI. All cryptographic algorithms must be FIPS-approved or recommended and the cryptographic module validated against FIPS 140, *Security Requirements for Cryptographic Modules* (References to FIPS 140 refer to the most recent version of the standard; the most recent version can be found at http://csrc.nist.gov/cryptval). Security Level 1 requires, at a minimum, two distinct roles. One role will be responsible for account administration, key generation, audit configuration and a second role responsible for issuing and revoking certificates. These responsibilities must be divided between two (or more) separate, mutually exclusive, roles. Security Level 1 should be achievable using currently available products. Security Level 1 differs from higher levels in several aspects; for example, all cryptographic functions to be performed by cryptographic modules must be validated only to FIPS 140 Security Level 1.

At Security Level 1, the CIMC is evaluated at the Common Criteria (CC) Evaluation Assurance Level (EAL) 1 with the addition of Functional testing. The objective of this assurance level is to provide evidence that the CIMC functions as specified in the associated documentation.

1.2.4.2 Security Level 2

CIMCs designed to meet Security Level 2 may be appropriate where the risks and consequences of data disclosure are not significant. CIMCs at Security Level 2 should defend against most attacks initiated through a network. It is assumed at this security level that the users of the PKI are not malicious. Security Level 2 requires, at a minimum, two distinct roles. One role will be responsible for account administration, key generation, audit configuration and a second role responsible for issuing and revoking certificates. These responsibilities must be divided between two (or more) separate, mutually exclusive, roles. Security Level 2 increases the number of events that must be audited and requires increased cryptographic protection of audit logs and system backups. In addition, FIPS 140 level 2 cryptographic modules are required for the protection of some private keying material.

At Security Level 2, the CIMC is evaluated against the assurance requirements specified in *CSPP – Guidance for COTS Security Protection Profiles.* The CSPP assurance level would be EAL3 except for Descriptive high-level design. It also adds Problem tracking configuration management coverage, Informal TOE security policy model, Flaw reporting procedures, and Validation of analysis components that are at the EAL4 level. The assurance requirements of CSPP stress assurance through vendor actions that are currently within best commercial practices.

1.2.4.3 Security Level 3

CIMCs designed to meet Security Level 3 may be appropriate for environments where risks and consequences of data disclosure and loss of data integrity are moderate. Level 3 requires additional integrity controls to ensure data is not modified. A CIMC at Security Level 3 includes protections to protect against someone with physical access to the components and includes additional assurance requirements to ensure the CIMC is functioning securely.

This security level provides some protection against malicious authorized users by requiring, at a minimum, three distinct roles. One role will be responsible for account administration, key generation, and audit configuration; a second role will be responsible for issuing and revoking certificates; and a third role responsible for maintaining the audit logs. Security Level 3 requires two-party control of private key export and additional auditing of import and export of secret and private keys and requests for information. Cryptographic modules responsible for long-term private key protection or for signing certificates or certificate status information must be validated to FIPS 140 Security Level 3. Finally, there is increased public key protection and digital signatures are required on all messages.

At Security Level 3, the applicable CC assurance requirements are extracted from EAL3 (methodically tested and checked) and EAL4 (methodically designed, tested and reviewed). The majority of the requirements are from EAL3. An EAL3 evaluation provides an analysis supported by “gray box” testing, selective independent confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. An EAL4 evaluation provides an analysis supported by the low-level design of the modules of the TOE, and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities.

1.2.4.4 Security Level 4

CIMCs designed to meet Security Level 4 may be appropriate where the threats to and consequences of data disclosure and loss of data integrity are significant. The environment and the users may be hostile. Security Level 4 is intended to protect against malicious authorized and unauthorized users. This is partly accomplished by requiring, at a minimum, four distinct roles. One role will be responsible for account administration and key generation; a second role responsible for maintaining the audit logs; a third role responsible for issuing and revoking certificates; and a fourth role responsible for performing backups. A Security Level 4 CIMC requires significant assurance that the security features are functioning properly. Security Level 4 increases the integrity of audit logs by requiring signed third-party timestamping. Cryptographic modules responsible for long-term private key protection or for signing certificates or certificate status information must be validated to FIPS 140 level 4. CIMC Security Level 4 products are currently not available, but should be achievable in the next few years.

At Security Level 4, the applicable CC assurance requirements are extracted from EAL4 (methodically designed, tested and reviewed) and EAL5 (semiformally designed and tested). The majority of the requirements are from EAL4. EAL5 permits a developer to gain maximum assurance from security engineering based on rigorous commercial development practices, supported by moderate application of specialized security engineering techniques.

1.2.5 Requirements Overview

All CIMCs must implement the mandatory requirements and functions. Requirements and functions that are not specifically marked as mandatory are optional. However, if a CIMC implements an optional function, the CIMC must implement the security requirements specified in the document for that function.

Security requirements are also separated according to the Security Level for which they are applicable. Unless otherwise specified, the security requirements in each subsection apply to all four Security Levels.

2 TOE DESCRIPTION

The CIMC Protection Profile (CIMC PP) defines a set of security requirements to be levied on Targets of Evaluation (TOEs). These TOEs include information systems that may include general purpose operating systems. A CIMC TOE may be a stand-alone system or consist of components in a network or distributed environment. A CIMC TOE permits one or more processors and associated peripherals and storage devices to be used by multiple users to perform a variety of PKI functions requiring controlled, shared access to the information stored on the system.

All individual users are assigned a unique identifier. This identifier supports individual accountability.

3 TOE SECURITY ENVIRONMENT

This section includes the following:

- Secure usage assumptions,
- Threats, and
- Organizational security policies.

This information provides the basis for the Security Objectives specified in Section 4, the Security Requirements for the IT Environment specified in Section 5, the TOE Security Functional Requirements specified in Section 6, and the TOE Security Assurance Requirements specified in Section 7.

3.1 Secure Usage Assumptions

The usage assumptions are organized in four categories: authorized users, system failures, cryptography, and external attacks.

Authorized Users

A.Auditors Review Audit Logs
Audit logs are required for security-relevant events and must be reviewed by the Auditors.

A.Competent Administrators, Operators, Officers and Auditors
Competent Administrators, Operators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.

A.Cooperative Users
Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner. (Levels 1–3).

A.No Abusive Administrators, Operators, Officers and Auditors
Administrators, Operators, Officers and Auditors are trusted not to abuse their authority. (Levels 1-2)

A.Social Engineering Training
General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks.

System Failures

A.Authentication Data Management
Authentication data management is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.)

A.Disposal of Authentication Data
Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).

A.Operating System
Operating systems are at the core of any IT system and must be chosen such that the security of the operating system is sufficient to safeguard against identified risks and threats.

External Attacks

A.Communications Protection
The system is adequately physically protected against loss of communications i.e., availability of communications.

A.Hardware Integrity
The system shall include integrity mechanisms to provide for the detection of hardware modifications.

A.Malicious Code Not Signed
Malicious code destined for the TOE is not signed by a trusted entity.

A.Physical Protection
The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.

3.2 Threats

The threats are organized in four categories: authorized users, system failures, cryptography and external attacks.

Authorized Users

T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
An Administrator, Operator, Officer or Auditor commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur. (Addressed at Levels 3-4, only)

T.Administrative errors of omission
Administrators, Operators, Officers or Auditors fail to perform some function essential to security.

T.User abuses authorization to collect and/or send data
User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data. (Abuse of authorization to collect data addressed at Levels 3-4, only)

T.User error makes data inaccessible
User accidentally deletes user data rendering user data inaccessible.

System Failures

T.Critical system component fails
Failure of one or more system components results in the loss of system critical functionality.

T.Flawed code
A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

T.Malicious code exploitation
An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets. (Addressed at Level 4, only)

T.Message content modification
A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.

T.TOE developed with inadequate TSF self protection
System or applications developer delivers code that includes security flaws that prevent the TSF from adequately protecting itself. The security flaws may be either deliberate or accidental.

Cryptography

T.Disclosure of private and secret keys
A private or secret key is improperly disclosed.

T.Modification of private/secret keys
A secret/private key is modified.

T.Sender denies sending information
The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction. (Addressed at Levels 3-4, only)

External Attacks

T.Hacker gains access
A hacker: masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

T.Hacker physical access
A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.

T.Social engineering
A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation. (Addressed at Levels 3-4, only)

3.3 Organizational Security Policies

P.Authorized use of information

Information shall be used only for its authorized purpose(s).

P.Cryptography
FIPS-approved or NIST-recommended cryptographic functions shall be implemented.

4 SECURITY OBJECTIVES

This section includes the security objectives for the CIMC PP including IT TOE security objectives, non-IT security objectives, and non-TOE IT security objectives.

4.1 Security Objectives for the TOE

This section includes the security objectives for the TOE, divided among four categories: authorized users, system failures, cryptography, and external attacks.

Authorized Users

O.Administrators, Operators, Officers and Auditors guidance documentation
Deter Administrator, Operator, Officer or Auditor errors by providing adequate documentation on securely configuring and operating the CIMC.

O.Certificates
The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid.

O.Detect modifications of firmware, software, and backup data
Provide integrity protection to detect modifications to firmware, software, and backup data.

O.Individual accountability and audit records
Provide individual accountability for audited events. Record in audit records: date and time of action and the entity responsible for the action.

O.Limitation of administrative access
Design administrative functions so that Administrators, Operators, Officers and Auditors do not automatically have access to user objects, except for necessary exceptions. Control access to the system by Operators and Administrators who troubleshoot the system and perform system updates.

O.Maintain user attributes
Maintain a set of security attributes (which may include role membership. access privileges, etc.) associated with individual users. This is in addition to user identity.

O.Respond to possible loss of stored audit records
Respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.

O.Restrict actions before authentication
Restrict the actions a user may perform before the TOE verifies the identity of the user.

O.Security roles
Maintain security-relevant roles and the association of users with those roles.

O.Security-relevant configuration management
Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.

O.User authorization management
Manage and update user authorization and privilege data to ensure they are consistent with organizational security and personnel policies.

System Failures

O.Configuration Management
Implement a configuration management plan. Implement configuration management to assure identification of system connectivity (software, hardware, and firmware), and components (software, hardware, and firmware), auditing of configuration data, and controlling changes to configuration items.

O.Examine source code for developer flaws
Examine for accidental or deliberate flaws in code made by the developer. The deliberate flaws include building trap doors. (Addressed at Level 4, only)

O.Integrity protection of user data and software
Provide appropriate integrity protection for user data and software.

O.Lifecycle security
Provide tools and techniques used during the development phase to ensure security is designed into the CIMC. Detect and resolve flaws during the operational phase. (Addressed at Level 2 – 4)

O.Manage behavior of security functions
Provide management functions to configure, operate, and maintain the security mechanisms.

O.Object and data recovery free from malicious code
Recover to a viable state after malicious code is introduced and damage occurs. That state must be free from the original malicious code.

O.Periodically check integrity
Provide periodic integrity checks on both system and software.

O.Preservation/trusted recovery of secure state
Preserve the secure state of the system in the event of a secure component failure and/or recover to a secure state.

O.Procedures for preventing malicious code
Incorporate malicious code prevention procedures and mechanisms.

O.Protect stored audit records
Protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.

O.Protect user and TSF data during internal transfer
Ensure the integrity of user and TSF data transferred internally within the system.

O.Repair identified security flaws.
The vendor repairs security flaws that have been identified by a user.

O.Require inspection for downloads
Require inspection of downloads/transfers.

O.Sufficient backup storage and effective restoration
Provide sufficient backup storage and effective restoration to ensure that the system can be recreated.

O.Time stamps

Provide time stamps to ensure that the sequencing of events can be verified.

O.Validation of security function
Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.

Cryptography

O.Cryptographic functions
The TOE must implement approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and use validated cryptographic modules. (Validated is defined as FIPS 140 validated.)

O.Non-repudiation
Prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message. (Assurance provided at Levels 3 and 4.)

External Attacks

O.Control unknown source communication traffic
Control (e.g., reroute or discard) communication traffic from an unknown source to prevent potential damage.

O.Data import/export
Protect data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.

O.General user documentation
Provide documentation for the general user and for the administrative roles.

O.React to detected attacks
Implement automated notification (or other responses) to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent. (Addressed at Levels 2-4, only)

O.Trusted Path
Provide a trusted path between the user and the system. Provide a trusted path to security-relevant (TSF) data in which both end points have assured identities. (Addressed at Levels 3-4, only)

4.2 Non-IT Security Objectives

O.Administrative Training
Administrators, Operators, Officers and Auditors are trained to define, implement, and maintain effective security practices.

O.Auditors Review Audit Logs
Identify and monitor security-relevant events by requiring auditors to review audit logs on a frequency sufficient to address level of risk.

O.Competent Administrators, Operators, Officers and Auditors
Provide capable management of the TOE by assigning competent Administrators, Operators, Officers and Auditors to manage the TOE and the security of the information it contains.

O.Cooperative Users
Ensure that users are cooperative so that they can accomplish some task or group of tasks that require a secure IT environment and information managed by the TOE. (Levels 1–3).

O.CPS
All Administrators, Operators, Officers and Auditors shall be familiar with the certificate policy (CP) and the certification practice statement (CPS) that describes the TOE.

O.Credentials
Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner that maintains IT security.

O.Disposal of Authentication Data
Provide proper disposal of authentication data and associated privileges after access has been removed (e.g., job termination, change in responsibility).

O.Installation
Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.

O.No Abusive Administrators, Operators, Officers and Auditors
Use trustworthy Administrators, Operators, Officers and Auditors. (Levels 1-2)

O.Notify authorities of security issues
Notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.

O.Physical Protection
Those responsible for the TOE must ensure that the security-relevant components of the TOE are protected from physical attack that might compromise IT security.

O.Social Engineering Training
Provide training for general users, administrators, operators, officers and auditors in techniques to thwart social engineering attacks.

4.3 Non-TOE IT Security Objectives

O.Authentication Data Management
Ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) through enforced authentication data management (Note: this objective is not applicable to biometric authentication data.)

O.Communications Protection
Protect the system against a physical attack on the communications capability by providing adequate physical security.

O.Hardware Integrity
Provide integrity mechanisms to enable detection of hardware modifications.

O.Malicious Code Not Signed
Protect the TOE from malicious code by ensuring all code is signed by a trusted entity prior to loading it into the system.

O.Operating System
The operating system used provides adequate security and meets security requirements recommended by the National Institute of Standards and Technology.

5 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

Users cannot bypass the security mechanisms of the TOE. The underlying system will provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with.

Software sent from outside sources must be handled to protect against the inclusion of unauthorized software, for example, viruses and Trojan horses.

Provide through frequent audits, restoration of security-relevant changes to the system between backup and restore, and restoration of the security-relevant system state (e.g., access control list) without destruction of other system data.

Provide through frequent backups, restoration of system changes between backup and restore.
Every CIMC will have a certification practice statement (CPS) and a certificate policy (CP) that documents the operation of the CIMC.

6 TOE SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the security requirements that are applicable to CIMC functionality, such as key management, certificate registration, and CIMC configuration and management functions. The CIMC requirements are specified by level. If a requirement is listed without levels, the requirement applies to all four levels.

Table 1 lists all the CC functional security requirements that are included in this PP. They are listed in alphabetical order in Table 1 for ease of reference. Also included is the applicable CIMC PP section.

Table 1. CIMC Functional Security Requirements

CC Functional Requirement	CIMC PP Section
FAU_GEN.1 Audit data generation	6.1 Security Audit
FAU_GEN.2 User identity association	6.1 Security Audit
FAU_SAR.1 Audit Review	6.1 Security Audit
FAU_SAR.3 Selectable audit review	6.1 Security Audit
FAU_SEL.1 Selective audit	6.1 Security Audit
FAU_STG.1 Protected audit trail storage	6.1 Security Audit
FAU_STG.4 Prevention of audit data loss	6.1 Security Audit
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	6.6 Remote Data Entry and Export
FCO_NRO_CIMC.4 Advanced verification of origin	6.6 Remote Data Entry and Export
FCS_CKM.1 Cryptographic key generation	6.7 Key Management
FCS_CKM.4 Cryptographic key destruction	6.7 Key Management
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	6.7 Key Management
FCS_COP.1 Cryptographic operation	6.14 Cryptographic Modules
FDP_ACC.1 Security attribute based access control	6.4 Access Control
FDP_ACF.1 Security attribute based access control	6.4 Access Control
FDP_ACF_CIMC.2 User private key confidentiality protection	6.7 Key Management
FDP_ACF_CIMC.3 User secret key confidentiality protection	6.7 Key Management
FDP_CIMC_BKP.1 CIMC backup and recovery	6.3 Backup and Recovery
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	6.3 Backup and Recovery
FDP_CIMC_BKP.3 Advanced CIMC backup and recovery	6.3 Backup and Recovery
FDP_CIMC_CER.1 Certificate Generation	6.12 Certificate Registration
FDP_CIMC_CRL.1 Certificate Revocation	6.13 Certification Revocation
FDP_CIMC_CSE.1 Certificate status export	6.6 Remote Data Entry and Export
FDP_CIMC_OCSP.1 Basic Response Validation	6.13 Certificate Revocation

Table 1. CIMC Functional Security Requirements

CC Functional Requirement	CIMC PP Section
FDP_CIMC_POP.1 Proof of possession for key management keys	6.12 Certificate Registration
FDP_ETC_CIMC.4 User private and secret key export	6.7 Key Management
FDP_ETC_CIMC.5 Extended user private and secret key export	6.7 Key Management
FDP_ITT.1 Basic internal transfer protection	6.6 Remote Data Entry and Export
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	6.7 Key Management
FDP_UCT.1 Basic data exchange confidentiality	6.6 Remote Data Entry and Export
FIA_AFL.1 Authentication failure handling	6.5 Identification and Authentication
FIA_ATD.1 User attribute definition	6.5 Identification and Authentication
FIA_UAU.1 Timing of authentication	6.5 Identification and Authentication
FIA_UID.1 Timing of identification	6.5 Identification and Authentication
FIA_USB.1 User-subject binding	6.5 Identification and Authentication
FMT_MOF.1 Management of security functions behavior	6.2 Roles
FMT_MOF_CIMC.2 Certificate profile management	6.9 Certificate Profile Management
FMT_MOF_CIMC.3 Extended certificate profile management	6.9 Certificate Profile Management
FMT_MOF_CIMC.4 Certificate revocation list profile management	6.10 Certificate Revocation List Profile Management
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	6.10 Certificate Revocation List Profile Management
FMT_MOF_CIMC.6 OCSP Profile Management	6.11 Online Certificate Status Protocol (OCSP) Profile Management
FMT_MSA.1 Management of security attributes	6.2 Roles
FMT_MSA.2 Secure security attributes	6.2 Roles
FMT_MSA.3 Static attribute initialization	6.2 Roles
FMT_MTD.1 Management of TSF data	6.2 Roles
FMT_MTD_CIMC.4 TSF private key confidentiality protection	6.7 Key Management
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	6.7 Key Management
FMT_MTD_CIMC.6 TSF private and secret key export	6.7 Key Management
FMT_MTD_CIMC.7 Extended TSF private and secret key export	6.7 Key Management
FMT_SMR.2 Restrictions on security roles	6.2 Roles
FPT_AMT.1 Abstract machine testing	6.8 Self Tests
FPT_CIMC_TSP.1 Audit log signing event	6.1 Security Audit
FPT_CIMC_TSP.2 Audit log time stamp event	6.1 Security Audit
FPT_ITC.1 Inter-TSF confidentiality during transmission	6.6 Remote Data Entry and Export
FPT_ITT.1 Basic internal TSF data transfer protection	6.6 Remote Data Entry and Export
FPT_STM.1 Reliable time stamps	6.1 Security Audit
FPT_TST_CIMC.2 Software/firmware integrity test	6.8 Self Tests
FPT_TST_CIMC.3 Software/firmware load test	6.8 Self Tests
FTP_TRP.1 Trusted path	6.5 Identification and Authentication

6.1 Security Audit (Mandatory)

Audit includes a chronological recording of events that occur in a system. The objective is to track what occurs to enable the reconstruction and examination of a sequence of events and/or changes in an event. This is useful in ensuring that the system is operated securely and in providing evidence when a suspected or actual security compromise has occurred. Audit also provides for reconstructing a specific state of a system. The objective in a PKI system is to enable an appropriate authority to determine whether a signature should have been accepted as valid.

The audit will be used to reconstruct important events that were performed by the CIMC, such as issuance of a CA certificate, and the user or event (e.g., a signed certificate request) that caused them. The audit will be used to arbitrate future disputes by establishing the validity of a signature at a particular time.

The audit log records the security-relevant events that were performed by the CIMC and the users or events (e.g., a signed certificate request) that caused them. This subsection specifies the security requirements for maintaining and protecting the integrity of the audit logs. If the audit requirements are addressed by the underlying operating system, they do not need to be separately addressed by the CIMC.

The CIMC may maintain either a single audit log or multiple audit logs. If multiple audit logs are used, the CIMC may either maintain a different audit log at each of the physically separated parts of the CIMC (e.g., the CA may maintain an audit log in addition to each of the RAs) or may divide audit entries among the audit logs based on the type of event being audited (e.g., audit entries that are to be maintained for a very long time may be placed in a separate audit log to be used as an archive). If multiple audit logs are maintained, each event to be audited (as specified in FAU_GEN.1) must be included in at least on of the audit logs. All other audit requirements apply to each audit log.

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the basic level of audit; and

c) The events listed in Table 2 below.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, the information specified in the Additional Details column in Table 2 below.

FAU_GEN.1.3 The audit shall not include plaintext private or secret keys or other critical security parameters.

Dependencies: FPT_STM.1 Reliable time stamps

Table 2. Auditable Events and Audit Data

Section/Function	Component	Event	Additional Details
6.1: Security Audit	FAU_GEN.1 Audit data generation	Any changes to the audit parameters, e.g., audit frequency, type of event audited	
		Any attempt to delete the audit log	
	FPT_CIMC_TSP.1 Audit log signing event	Audit log signing event	Digital signature, keyed hash, or authentication code shall be included in the audit log.
	FPT_CIMC_TSP.2 Audit log time stamp event	Obtaining a third party time stamp	The digitally signed third party timestamp shall be included in the audit log.
6.5: Identification and Authentication	FIA_ATD.1 User attribute definition	Successful and unsuccessful attempts to assume a role	

Table 2. Auditable Events and Audit Data

Section/Function	Component	Event	Additional Details
	FIA_AFL.1 Authentication failure handling	The value of *maximum authentication attempts* is changed (Levels 2, 3, 4)	
		Maximum authentication attempts unsuccessful authentication attempts occur during user login (Levels 2, 3, 4)	
	FIA_AFL.1 Authentication failure handling	An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts (Levels 2, 3, 4)	
		An Administrator changes the type of authenticator, e.g., from password to biometrics (Levels 2, 3, 4)	
Local Data Entry		All security-relevant data that is entered in the system	The identity of the data entry individual if the entered data is linked to any other data (e.g., clicking an "accept" button). This shall be included with the accepted data.
Remote Data Entry		All security-relevant messages that are received by the system	
Data Export and Output		All successful and unsuccessful requests for confidential and security-relevant information (Levels 2, 3, 4)	
6.7.1: Key Generation	FCS_CKM.1 Cryptographic Key Generation	Whenever the CIMC generates a key. (Not mandatory for single session or one-time use symmetric keys.)	The public component of any asymmetric key pair generated
Private Key Load		The loading of Component private keys	
6.7.2 Private Key Storage		All access to certificate subject private keys retained within the CIMC for key recovery purposes	
Trusted Public Key Entry, Deletion and Storage		All changes to the trusted public keys, including additions and deletions	The public key and all information associated with the key
6.7.4: Secret Key Storage		The manual entry of secret keys used for authentication (Levels 3 and 4)	
6.7.6: Private and Secret Key Export	FDP_ETC_CIMC.4 User private and	The export of private and secret keys (keys used for a	

Table 2. Auditable Events and Audit Data

Section/Function	Component	Event	Additional Details
	secret key export; FMT_MTD_CIMC.6 TSF private and secret key export	single session or message are excluded)	
6.12: Certificate Registration	FDP_CIMC_CER.1 Certificate Generation	All certificate requests	If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by Officer, etc.).
Certificate Status Change Approval		All requests to change the status of a certificate	Whether the request was accepted or rejected.
CIMC Configuration		Any security-relevant changes to the configuration of the CIMC	
Account Administration		Roles and users are added or deleted	
		The access control privileges of a user account or a role are modified	
6.9: Certificate Profile Management	FMT_MOF_CIMC.2 Certificate profile management; FMT_MOF_CIMC.3 Extended certificate profile management	All changes to the certificate profile	The changes made to the profile
Revocation Profile Management		All changes to the revocation profile	The changes made to the profile
6.10: Certificate Revocation List Profile Management	FMT_MOF_CIMC.4 Certificate revocation list profile management; FMT_MOF_CIMC.5 Extended certificate revocation list profile management	All changes to the certificate revocation list profile	The changes made to the profile
6.11: OCSP Profile Management	FMT_MOF_CIMC.6 OCSP Profile Management	All changes to the OCSP profile	The changes made to the profile

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide *Auditors* with the capability to read [ST assignment: *list of audit information*] from the audit records.

Application Note: The ST author should specify the type of information the specified user is permitted to obtain from the audit records. Examples are "all", "subject identity", "all information belonging to audit records referencing this user".

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform searches of audit data based on the type of event, the ability of the user responsible for causing the event, and as specified in Table 3 below.

Dependencies: FAU_SAR.1 Audit review

Table 3. Audit Search Criteria

Section/Function	Component	Search Criteria
Certificate Request Remote and Local Data Entry		Identity of the subject of the certificate being requested
Certificate Revocation Request Remote and Local Data Entry		Identity of the subject of the certificate to be revoked

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [selection: *object identity, user identity, subject identity, host identity, event type]*

b) [assignment: *list of additional attributes that audit selectivity is based upon]*.

Application Note: The ST must state the events that may be included or excluded and must indicate the attributes used in this determination.

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent modifications to the audit records.

Dependencies: FAU_GEN.1 Audit data generation

NOTE: One method of meeting the requirements of FAU_STG.1 is to write audit data directly to non-modifiable media.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by the Auditor, if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies.

SECURITY LEVELS 2 and 3

In addition to the above security requirements, FPT_CIMC_TSP.1 shall apply to CIMCs at Security Levels 2 and 3.

FPT_CIMC_TSP.1 Audit log signing event

Hierarchical to: No other components.

FPT_CIMC_TSP.1.1 The TOE shall periodically create an audit log signing event in which it computes a digital signature, keyed hash, or authentication code over the entries in the audit log.

FPT_CIMC_TSP.1.2 The digital signature, keyed hash, or authentication code shall be computed over, at least, every entry that has been added to the audit log since the previous audit log signing event and the digital signature, keyed hash, or authentication code from the previous audit log signed event.

FPT_CIMC_TSP.1.3 The specified frequency at which the audit log signing event occurs shall be configurable.

FPT_CIMC_TSP.1.4 The digital signature, keyed hash, or authentication code from the audit log signing event shall be included in the audit log.

Dependencies: FAU_GEN.1

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by existing Common Criteria requirements. It supports the security objective O.Protect stored audit records, by providing additional protection for stored audit records at Security Levels 2 and 3.

SECURITY LEVEL 4

In addition to the above security requirements, FPT_CIMC_TSP.2 shall apply to CIMCs at Security Level 4.

FPT_CIMC_TSP.2 Audit log time stamp event

Hierarchical to: No other components.

FPT_CIMC_TSP.2.1 The TSF shall obtain a digitally signed third party timestamp at a specified frequency.

FPT_CIMC_TSP.2.2 The digital signature of the third party timestamp shall be computed over, at least, every entry that has been added to the audit log since the previous third party

timestamp was generated and the digital signature from the previous third party timestamp.

FPT_CIMC_TSP.2.3 The TOE shall not compute the digital signature.

FPT_CIMC_TSP.2.4 The specified frequency at which the TOE obtains a third party timestamp shall be configurable.

FPT_CIMC_TSP.2.5 The digitally signed third party timestamp shall be included in the audit log.

Dependencies: FAU_GEN.1

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by existing Common Criteria requirements. It supports the security objective O.Time Stamps, by ensuring that modifications to the audit logs can be detected.

6.2 Roles (Mandatory)

The ability to perform many of the functions specified in this PP will be allocated to distinct roles to maintain the security of a CIMC. This subsection defines a set of roles that will be used throughout this document when allocating responsibilities.

A CIMC is not required to implement all of the roles listed, but is only required to implement roles to meet the role separation requirements. A single identity may be assigned multiple roles except where prohibited by the CIMC requirements. Multiple individuals may be assigned to a specific role, as required by the CIMC implementation.

The role definitions are listed below:

1. *Administrator* – role authorized to install, configure, and maintain the CIMC; establish and maintain user accounts; configure profiles and audit parameters; and generate Component keys.
2. *Operator* – role authorized to perform system backup and recovery.
3. *Officer* – role authorized to request or approve certificates or certificate revocations.
4. *Auditor* – role authorized to view and maintain audit logs.

It is important that one individual cannot perform all the functions specified for a CIMC. One mechanism to deter abuse of power is the separation of CA duties.

FMT_SMR.2 Restrictions on security roles

Hierarchical to: FMT_SMR.1

FMT_SMR.2 has different requirements for security levels 1 and 2, security level 3, and security level 4.

SECURITY LEVELS 1 AND 2

FMT_SMR.2.1 The TSF shall maintain the roles Administrator and Officer.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that no identity is authorized to assume both an Administrator and an Officer role.

SECURITY LEVEL 3

FMT_SMR.2.1 The TSF shall maintain the roles Administrator, Auditor, and Officer.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that:

a) no identity is authorized to assume both an Administrator and an Officer role;

b) no identity is authorized to assume both an Auditor and an Officer role; and

c) no identity is authorized to assume both an Administrator and an Auditor role.

SECURITY LEVEL 4

FMT_SMR.2.1 The TSF shall maintain the roles Administrator, Auditor, Officer, and Operator.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that no identity is authorized to assume more than one of the role specified above.

Dependencies: FIA_UID.1 Timing of identification

NOTE: If a CIMC does not implement one of the roles specified above (e.g., Auditor or Operator), then the capabilities assigned to that role by this Protection Profile must be assigned to some other role or roles.

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions listed in Table 4 to the authorized roles.

Dependencies: FMT_SMR.1 Security roles

Table 4. Authorized Roles for Management of Security Functions Behavior

Section/Function	Component	Event
6.1: Security Audit		The capability to configure the audit parameters shall be restricted to Administrators. The capability to change the frequency of the audit log signing event shall be restricted to Administrators. (Levels 2-4). The capability to change the frequency of the timestamping event or the source of the timestamp shall be restricted to Administrators. (Level 4)
6.3: Backup and Recovery		The capability to configure the backup parameters shall be restricted to Administrators. The capability to initiate the backup or recovery function shall be restricted to Operators.
6.5: Identification and Authentication		The capability to specify or change *maximum authentication attempts* shall be restricted to Administrators. The capability to change authentication mechanisms shall be restricted to Administrators.
6.12: Certificate Registration		The capability to approve fields or extensions to be included in a certificate shall be restricted to Officers. If an automated process is used to approve fields or extensions to be included in a certificate, the capability to configure that process shall be restricted to Officers.

Table 4. Authorized Roles for Management of Security Functions Behavior

Section/Function	Component	Event
Data Export and Output		Private key export shall be performed by the Administrator (Security Levels 1 and 2). The export of CIMC private keys shall require the authorization of at least two Administrators or one Administrator and one Officer, Auditor, or Operator. (Security Levels 3 and 4)
Certificate Status Change Approval		Only Officers shall configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate. Only Officers shall configure the automated process used to approve the placing of a certificate on hold or information about the on hold status of a certificate.
CIMC Configuration		The capability to configure any CIMC functionality shall be restricted to Administrators. (This requirement applies to all configuration parameters unless the ability to configure that aspect of the CIMC functionality has been assigned to a different role elsewhere in this document.)
Account Administration		The capability to create user accounts and roles shall be restricted to Administrators. The capability to assign privileges to those accounts and roles shall be restricted to Administrators.
6.9: Certificate Profile Management	FMT_MOF_CIMC.2 Certificate profile management; FMT_MOF_CIMC.3 Extended certificate profile management	The capability to modify the certificate profile shall be restricted to Administrators.
Revocation Profile Management		The capability to modify the revocation profile shall be restricted to Administrators.
6.10: Certificate Revocation List Profile Management	FMT_MOF_CIMC.4 Certificate revocation list profile management; FMT_MOF_CIMC.5 Extended certificate revocation list profile management	The capability to modify the certificate revocation list profile shall be restricted to Administrators.
6.11: OCSP Profile Management	FMT_MOF_CIMC.6 OCSP profile management	The capability to modify the OCSP profile shall be restricted to Administrators.

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the CIMC access control policy to restrict the ability to modify the security attributes [ST assignment: *list of security attribute*s] to Administrators.

Application Note: The ST must state components of the security attributes that may be modified and any restrictions that may exist for Administrators. The ST must state the components of the access rights that the Administrator is allowed to modify.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the CIMC access control policy to provide [ST selection: *restrictive, permissive, other property*] default values for security attributes that are used to enforce the SFP.

Application Note: The TSF shall provide default values for relevant object security attributes, which can be overridden by an initial value. It may be possible for a new object to have different security attributes at creation, if a mechanism exists to specify the permissions at time of creation. The ST author should select whether the default property of the access control attribute will be restrictive, permissive, or another property. In case of another property, the ST author should refine this to a specific property.

FMT_MSA.3.2 The TSF shall allow the Administrator to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

SECURITY LEVELS 2, 3, AND 4

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security Roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to view (read) or delete the audit logs to Auditors.

Dependencies: FMT_SMR.1 Security roles

6.3 Backup and Recovery (Mandatory)

Backup and recovery includes reconstructing a system in the event of a system failure or other serious error.

In order to be able to recover from failures and other unanticipated undesired events, CIMCs must be able to back up the system. The backup will be used to restore the CIMC to an operational status at a previous point in time. The frequency of performing backups (e.g., hourly, daily, or weekly) is based on the

criticality of the application or system. The backup and recovery requirements may be addressed by the underlying CIMC operating system.

FDP_CIMC_BKP.1 CIMC backup and recovery

Hierarchical to: No other components.

FDP_CIMC_BKP.1.1 The TSF shall include a backup function.

FDP_CIMC_BKP.1.2 The Operator shall be capable of invoking the backup function on demand.

FDP_CIMC_BKP.1.3 The data stored in the system backup shall be sufficient to recreate the state of the system at the time the backup was created using only:

i. a copy of the same version of the CIMC as was used to create the backup data;

ii. a stored copy of the backup data;

iii. the cryptographic key(s), if any, needed to verify the digital signature, keyed hash, or authentication code protecting the backup; and

iv. the cryptographic key(s), if any, needed to decrypt any encrypted critical security parameters.

FDP_CIMC_BKP.1.4 The TSF shall include a recovery function that is able to restore the state of the system from a backup.[1]

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objectives O.Object and data recovery free from malicious code and O.Preservation/trusted recovery of secure state.

SECURITY LEVELS 2 and 3

In addition to the above requirements, FDP_CIMC_BKP.2 shall apply to CIMCs at Security Levels 2 and 3.

FDP_CIMC_BKP.2 Extended CIMC backup and recovery

Hierarchical to: No other components.

FDP_CIMC_BKP.2.1 The backup data shall be protected against modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_CIMC_BKP.2.2 Critical security parameters and other confidential information shall be stored in encrypted form only.

Dependencies: FDP_CIMC_BKP.1 CIMC backup and recovery

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objectives O.Object and data recovery free from malicious code and O.Preservation/trusted recovery of secure state.

SECURITY LEVEL 4

[1] NOTE: The recovery function, in restoring the state of the system, is only required to create an "equivalent" system state in which information about all relevant CIMC transactions has been maintained.

In addition to the requirements at Security Levels 2 and 3, FDP_CIMC_BKP.3 shall apply to CIMCs at Security Level 4.

FDP_CIMC_BKP.3 Advanced CIMC backup and recovery

Hierarchical to: No other components.

FDP_CIMC_BKP.3.1 The TSF shall maintain sufficient information to recreate the state of the system at the time of the last completed CIMC transaction using only:

i. a copy of the same version of the CIMC as was used to create the backup data;

ii. a stored copy of the backup data from the most recently created system backup;

iii. any data maintained by the CIMC in non-volatile storage (e.g., magnetic disk or tape or other storage device whose contents are preserved when power is off);

iv. the cryptographic key(s), if any, needed to verify the digital signature, keyed hash, or authentication code protecting the backup; and

v. the cryptographic key(s), if any, needed to decrypt any encrypted critical security parameters.

FDP_CIMC_BKP.3.2 The recovery function of the TSF shall be capable of recreating the state of the system at the time of the last completed transaction. The recovery function shall reflect only completed transactions.

Dependencies: FDP_CIMC_BKP.1 CIMC backup and recovery
FDP_CIMC_BKP.2 Extended CIMC backup and recovery

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objectives O.Object and data recovery free from malicious code and O.Preservation/trusted recovery of secure state.

6.4 Access Control (Mandatory)

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the CIMC access control policy on [assignment: *list of subject*s, *objects, and operations among subjects and objects covered by the SF*P].

Application Note: The terms object and subject refer to generic elements in the TOE. For a policy to be implementable, these entities must be clearly identified. For most systems there is only one type of subject, usually called a process or task, which needs to be specified in the ST. For a PP, the objects and operations might be expressed as types such as: named objects, data repositories, observe accesses, etc. The ST author should specify the list of subjects, objects, and operations among subjects and objects covered by the SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the CIMC access control policy to objects based on the identity of the subject and the set of roles that the subject is authorized to assume.

FDP_ACF.1.2 The TSF shall enforce the rules specified in Table 5 to determine if an operation among controlled subjects and controlled objects is allowed.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [ST assignment: *rules, based on security attributes, that explicitly authorize access of subjects to object*s].

Application Note: The rules that govern the CIMC access control policy may vary between TOEs; those rules need to be specified in the ST. The ST must list the attributes that are used for access decisions. These attributes may include permission bits, access control lists, and object ownership. The ST author should specify the rules, based on security attributes, that explicitly **authorize** access of subjects to objects. These rules are in addition to those specified in FDP_ACF.1.1. They are included in FDP_ACF.1.3 as they are intended to contain exceptions to the rules in FDP_ACF.1.1.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [ST assignment: *rules, based on security attributes that explicitly deny access of subjects to object*s].

Application Note: The rules that govern the CIMC access control policy may vary between TOEs; those rules need to be specified in the ST. The ST must list the attributes that are used for access decisions. These attributes may include permission bits, access control lists, and object ownership. The ST author should specify the rules, based on security attributes, that explicitly **deny** access of subjects to objects. These rules are in addition to those specified in FDP_ACF.1.1. They are included in FDP_ACF.1.4 as they are intended to contain exceptions to the rules in FDP_ACF.1.1.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

Table 5. Access Controls

Section/Function	Component	Event
Certificate Request Remote and Local Data Entry		The entry of certificate request data shall be restricted to Officers and the subject of the requested certificate.
Certificate Revocation Request Remote and Local Data Entry		The entry of certificate revocation request data shall be restricted to Officers and the subject of the certificate to be revoked.
Data Export and Output		The export or output of confidential and security-relevant data shall only be at the request of authorized users.
6.7.1: Key Generation	FCS_CKM.1 Cryptographic Key Generation	The capability to generate Component keys (used to protect data in more than a single session or message) shall be restricted to Administrators.
Private Key Load		The capability to load Component private keys into cryptographic modules shall be restricted to Administrators.
6.7.2: Private Key Storage		The capability to decrypt certificate subject private keys within a CIMC shall be restricted to Officers. The TSF shall not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures. At least two Officers or one officer and an administrator, auditor, or operator shall be required to

Table 5. Access Controls

Section/Function	Component	Event
		decrypt certificate subject private keys. (Security Levels 3 and 4)
Trusted Public Key Entry, Deletion, and Storage		The capability to change (add, revise, delete) the trusted public keys shall be restricted to Administrators.
6.7.4: Secret Key Storage		The capability to load CIMC secret keys into cryptographic modules shall be restricted to Administrators.
6.7.5: Private and Secret Key Destruction		The capability to zeroize CIMC plaintext private and secret keys shall be restricted to Administrators, Auditors, Officers, and Operators.
6.7.6: Private and Secret Key Export		The capability to export a component private key shall be restricted to Administrators. The capability to export certificate subject private keys shall be restricted to Officers. The export of a certificate subject private key shall require the authorization of at least two Officers or one officer and an administrator, auditor, or operator. (Levels 3 and 4) (See note below)
Certificate Status Change Approval[2]		Only Officers and the subject of the certificate shall be capable of requesting that a certificate be placed on hold. Only Officers shall be capable of removing a certificate from on hold status. Only Officers shall be capable of approving the placing of a certificate on hold. Only Officers and the subject of the certificate shall be capable of requesting the revocation of a certificate. Only Officers shall be capable of approving the revocation of a certificate and all information about the revocation of a certificate.

6.5 Identification and Authentication (I&A) (Mandatory)

Identification and authentication includes recognizing an entity (e.g., user, device, or system) and verifying the identity of that entity. The I&A requirements may be addressed by the underlying CIMC operating system.

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

[2] Every request to change certificate status, for example, revoke a certificate, place a certificate on hold, or remove a certificate from hold must be accepted or rejected. If a request is accepted, any information about the request that may be exported from the CIMC must be approved. Approval may be manual or automated.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: the set of roles that the user is authorized to assume, [ST assignment: *other security attributes*].

Application Note: The specified attributes are those that are required by the TSF to enforce the CIMC access control policy, the generation of audit records, and proper identification and authentication of users. The user identity must be uniquely associated with a single individual user. Group membership may be expressed in a number of ways: a list per user specifying to which groups the user belongs, a list per group which includes which users are members, or implicit association between certain user identities and certain groups. The ST author should specify the security attributes that are associated with an individual user. An example of such a list is {'clearance, 'group identifier', 'rights'}.

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [ST assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [ST assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

Application Note: FIA_UAU.1 and FIA_UID.1 allow the ST author to specify TSF-mediated actions that may be performed on behalf of a user before that user is identified and/or authenticated. However, the TOE shall not perform any security-relevant functions or export/output any confidential information on behalf of a user before that user has been identified or authenticated. Examples of TSF-mediated actions that may be performed on behalf of a user before that user is identified and/or authenticated include:

a) Responding to a request for public information (e.g., responding to an Online Certificate Status Protocol (OCSP) request).

b) Accepting data from a user that will not be processed until an (identified and authenticated) authorized user has accepted the data (e.g., a unauthenticated user may submit a certificate request message so long as the certificate is not generated until after an Officer has approved the request).

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Dependencies: FIA_ATD.1 User attribute definition

SECURITY LEVEL 2

In addition to the I&A requirements specified above, FIA_AFL.1 shall also apply for Security Level 2.

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable *maximum authentication attempts* unsuccessful authentication attempts have occurred since the last successful authentication for the indicated user identity.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [ST assignment: *list of action*s].

Application Note: The ST must specify the actions to be taken in case the threshold is met or surpassed. These actions could be disabling of an account for five minutes or disabling of the account until unlocked by the administrator and simultaneously informing the administrator. (In order to prevent a denial-of-service attack, accounts that belong to Administrators should not be disabled.) The actions should specify the measures and, if applicable, the duration of the measure (or the conditions under which the measure will be ended).

Dependencies: FIA_UAU.1 Timing of authentication

SECURITY LEVELS 3 AND 4

In addition to the I&A requirements specified for Security Levels 1 and 2, FTP_TRP.1 shall apply for Security Levels 3 and 4.

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [ST selection: *local, local and remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit [ST selection: *the TSF, local users, remote user*s] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication, [ST assignment: *other services for which trusted path is require*d].

Application Note: The ST should identify other services for which a trusted path is required, if any. A trusted path may be required for any security-relevant interaction.

Dependencies: No dependencies

6.6 Remote Data Entry and Export

This section covers cases in which data is to be associated with a user who is not acting locally. In most cases, this will involve data that has been received in a message that has been signed or that contains an authentication code or keyed hash allowing the source of the message to be determined (in which case the data may be associated with the source of the message). Data received over a secure communication channel (e.g., SSL) could be treated similarly.

The security requirements of remote data entry apply whenever data has been received from a remote source that is considered reliable (i.e., the source of the information can be determined). These requirements also apply to communications between physically distributed parts of a single CIMC over an

untrusted network (e.g., receipt of a signed certificate request message by a CA from an RA would be considered a message receipt even if the RA and CA were being validated as a single CIMC).

This section also specifies security requirements associated with the export of data from CIMCs. The data may be distributed to a device that is outside the boundary of a CIMC (either locally or remotely). The remote device or computer may not be directly connected to the CIMC. Data export also applies when data is sent between physically distributed subcomponents of a CIMC (e.g., data sent between a CA and RA) and the data is transmitted over an untrusted network. Data export does not apply to data sent to a printer or monitor that is inside the CIMC boundary.

FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin

Hierarchical to: FCO_NRO.2

FCO_NRO_CIMC.3.1 The TSF shall enforce the generation of evidence of origin for certificate status information and all other security-relevant information at all times.

FCO_NRO_CIMC.3.2 The TSF shall be able to relate the identity and [ST assignment: *other attributes*] of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

Application Note: The ST shall specify the list of other attributes that shall be linked to the information, for example, time of origin and location of origin.

FCO_NRO_CIMC.3.3 The TSF shall verify the evidence of origin of information for all security-relevant information.

Dependencies: FIA_UID.1 Timing of identification

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by existing Common Criteria requirements. It supports the security objective O.Non-repudiation and O.Control unknown source communication traffic.

NOTE: Based on FCO_NRO_CIMC.3, the TSF shall reject any information whose origin can not be verified unless:

a) Acceptance of the information will not cause the TSF to perform any security relevant functions; and

b) Acceptance of the data will not cause the TSF to output or export any confidential information.

The TSF may, for example, accept information whose origin can not be verified under in the following cases:

a) The received information is a request for public information (e.g., an Online Certificate Status Protocol (OCSP) request).

b) The received information will not be processed until an authorized user has accepted its contents (e.g., a certificate request). In this case, the received information may be processed as if it had originated from the authorized user who approved it.

FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the CIMC access control policy to prevent the modification of security-relevant user data and the disclosure of confidential user data when it is transmitted between physically-separated parts of the TOE.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

FDP_UCT.1.1 The TSF shall enforce the CIMC access control policy to be able to transmit objects in a manner protected from unauthorized disclosure.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

FPT_ITC.1.1 The TSF shall protect confidential TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Dependencies: No dependencies

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1 The TSF shall protect security-relevant TSF data from modification when it is transmitted between separate parts of the TOE.

FPT_ITT.1.1 The TSF shall protect confidential TSF data from disclosure when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

SECURITY LEVELS 3 AND 4

In addition to the above Remote Data Entry and Export requirements, FCO_NRO_CIMC.4 shall apply to CIMCs at Security Levels 3 and 4.

FCO_NRO_CIMC.4 Advanced verification of origin

Hierarchical to: No other components.

FCO_NRO_CIMC.4.1 The TSF shall, for initial certificate registration messages sent by the certificate subject, only accept messages protected using an authentication code, keyed hash, or digital signature algorithm.

FCO_NRO_CIMC.4.2 The TSF shall, for all other security-relevant information, only accept the information if it was signed using a digital signature algorithm.

Dependencies: FCO_NRO_CIMC.3

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by existing Common Criteria requirements. It supports the security objective O.Non-repudiation.

6.6.1 Certificate Status Export (Mandatory)

All CIMCs must be capable of exporting certificate status information. Any message sent by a CIMC containing certificate status information must meet the requirements for Certificate Status Export in addition to the requirements for Data Export specified in section 6.6.

The following requirements apply to Certificate Status Export.

FDP_CIMC_CSE.1 Certificate status export

Hierarchical to: No other components

FDP_CIMC_CSE.1.1 If a message indicates the status of a certificate and the certificate is within its period of validity, then the message shall indicate the certificate's current status (e.g., valid, revoked, on hold).

FDP_CIMC_CSE.1.2 The status of a certificate shall be valid unless a change in status has been approved.

FDP_CIMC_CSE.1.3 If certificate status is output on a certificate revocation list (CRL), then the CRL shall be compliant with the X.509 standard.

FDP_CIMC_CSE.1.4 If certificate status is output as an Online Certificate Status Protocol (OCSP) response, then the OCSP response shall be compliant with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2560.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.7 Key Management

Cryptographic keys are used by CIMCs for many different reasons: to ensure the integrity of messages sent over untrusted networks, to authenticate users, to protect the confidentiality of private information, and to protect the confidentiality of stored information such as audit logs. As such, the unauthorized modification, disclosure, or substitution of any of these cryptographic keys could result in a loss of security.

Keys have a life cycle that begins with their generation. After generation, keys are stored, activated, deactivated, and destroyed. In many cases, keys are backed up and audited. Typically, public keys are distributed. In some cases, private and secret keys are distributed.

6.7.1 Key Generation (Mandatory)

This subsection specifies the requirements for the generation of cryptographic keys by CIMCs.

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in a cryptographic module that is in a FIPS-approved or recommended mode of operation. Certificate subject private keys shall be generated by a cryptographic module that meets the overall Security Level specified for Long Term Private Key Protection Keys (see Table 6). All other cryptographic keys shall be generated by a cryptographic module that meets the Security Level required for the use of the key (see Table 6).

Dependencies: [FCS_CKM.2 Cryptographic key distribution
or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

6.7.2 Private Key Storage (Mandatory)

Private keys may be used by a CIMC for many different purposes and stored for long periods. CIMCs may store Component keys, CIMS personnel keys, and, for key recovery purposes, certificate subject private keys.

FDP_ACF_CIMC.2 User private key confidentiality protection

Hierarchical to: No other components

FDP_ACF_CIMC.2.1 CIMS personnel private keys shall be stored in a cryptographic module or stored in encrypted form. If CIMS personnel private keys are stored in encrypted form, the encryption shall be performed by the TSF.

FDP_ACF_CIMC.2.2 If certificate subject private keys are stored in the CIMC, they shall be encrypted using a Long Term Private Key Protection Key. The encryption shall be performed by the TSF.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

FMT_MTD_CIMC.4 TSF private key confidentiality protection

Hierarchical to: No other components

FMT_MTD_CIMC.4.1 CIMC private keys shall be stored in a cryptographic module or stored in encrypted form. If CIMC private keys are stored in encrypted form, the encryption shall be performed by the TSF.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.7.3 Public Key Storage (Mandatory)

This subsection specifies security requirements that are designed to detect the unauthorized modification of public keys stored in a CIMC. The requirements in this section apply to CIMCs at Security Levels 3 and 4.

FDP_SDI_CIMC.3 Stored public key integrity monitoring and action

Hierarchical to: No other components

FDP_SDI_CIMC.3.1 Public keys stored within the TOE, but not within a FIPS 140 validated cryptographic module, shall be protected against undetected modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_SDI_CIMC.3.2 The digital signature, keyed hash, or authentication code used to protect a public key shall be verified upon each access to the key. If verification fails, the TSF shall [ST assignment: *action to be take*n].

Application Note: The ST should specify the actions to be taken in case the verification fails.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.7.4 Secret Key Storage

Secret (symmetric) keys may be used for several purposes in a CIMC. They may be used to encrypt other secret or private keys when they are stored within or exported from the CIMC. They may also be used to authenticate subscribers (users) and CIMCs. Secret keys must be protected against unauthorized modification and disclosure.

Applicants for certificates may be given PIN or password authenticators. The process for generating and delivering these authenticators to applicants is outside the scope of this document.

The following requirements are mandatory if the CIMC stores secret keys.

FDP_ACF_CIMC.3 User secret key confidentiality protection

Hierarchical to: No other components

FDP_ACF_CIMC.3.1 User secret keys stored within the TOE, but not within a FIPS 140 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the TSF.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

FMT_MTD_CIMC.5 TSF secret key confidentiality protection

Hierarchical to: No other components

FMT_MTD_CIMC.5.1 TSF secret keys stored within the TOE, but not within a FIPS 140 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the TSF.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.7.5 Private and Secret Key Destruction (Mandatory)

This section specifies requirements for the zeroization/destruction of plaintext private and secret keys stored within CIMCs.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [ST assignment: *cryptographic key destruction metho*d] that meets the following: [ST assignment: *list of standard*s].

Application Note: The ST should specify the key destruction method to be used to destroy cryptographic keys. The ST should specify the assigned standard that documents the method used to destroy cryptographic keys. The assigned standard may comprise none, one or more actual standards publications, for example, from international, national, industry or organizational standards.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

FCS_CKM_CIMC.5 CIMC private and secret key zeroization

Hierarchical to: No other components.

FCS_CKM_CIMC.5.1 The TSF shall provide the capability to zeroize plaintext secret and private keys within the TOE.

Dependencies: No dependencies.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.7.6 Private and Secret Key Export

Keys may be exported from cryptographic modules for a variety of reasons, including key backup, replication, and transmission of user private keys generated in CIMCs. There are different requirements for Security Levels 1 and 2 and Security Levels 3 and 4.

SECURITY LEVELS 1 AND 2

FDP_ETC_CIMC.4 User private and secret key export

Hierarchical to: No other components.

FDP_ETC_CIMC.4.1 Electronically distributed private and secret keys shall only be exported from CIMCs in encrypted form or using split knowledge procedures.

FDP_ETC_CIMC.4.2 Certificate subject private keys that are used to generate digital signatures shall not be exported from the CIMC in plaintext form.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

FMT_MTD_CIMC.6 TSF private and secret key export

Hierarchical to: No other components.

FMT_MTD_CIMC.6.1 Electronically distributed private and secret keys shall only be exported from CIMCs in encrypted form or using split knowledge procedures.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

NOTE: At Security Levels 1 and 2, manually distributed secret and private keys (other than certificate subject private keys that are used to generate digital signatures) may be exported in plaintext form from a CIMC.

SECURITY LEVELS 3 AND 4

FDP_ETC_CIMC.5 Extended user private and secret key export

Hierarchical to: FDP_ETC_CIMC.4

FDP_ETC_CIMC.5.1 Private and secret keys shall only be exported from CIMCs in encrypted form or using split knowledge procedures.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

FMT_MTD_CIMC.7 Extended TSF private and secret key export

Hierarchical to: FMT_MTD_CIMC.6

FMT_MTD_CIMC.7.1 Private and secret keys shall only be exported from CIMCs in encrypted form or using split knowledge procedures.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.8 Self-tests (Mandatory)

All CIMCs shall implement the following self-tests.

FPT_AMT.1 Abstract machine testing

Hierarchical to: No other components

FPT_AMT.1.1 The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorized user, other conditions*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Application Note: The ST author should specify when the TSF will execute the abstract machine testing. The ST author, through this selection, has the ability to indicate the frequency with which the self-tests will be run. If the tests are run often, then the end users should have more confidence that the TOE is operating correctly then if the tests are run less frequently. However, this must be balanced with the potential impact on the availability of the TOE.

Dependencies: No dependencies.

FPT_TST_CIMC.2 Software/firmware integrity test

Hierarchical to: No other components.

FPT_TST_CIMC.2.1 An error detection code (EDC) or FIPS-approved or recommended authentication technique (e.g., the computation and verification of an authentication code, keyed hash, or digital signature algorithm) shall be applied to all security-relevant software and firmware residing within the TOE (e.g., within EEPROM and RAM). The EDC shall be at least 16 bits in length.

FPT_TST_CIMC.2.2 The error detection code, authentication code, keyed hash, or digital signature shall be verified at power-up and on-demand. If verification fails, the TSF shall [ST assignment: *action to be taken*].

Application Note: The ST should specify the actions to be taken if signature verification fails.

Dependencies: FPT_AMT.1 Abstract machine testing.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria. It satisfies the security objective O.Integrity protection of user data and software and O.Periodically check integrity.

FPT_TST_CIMC.3 Software/firmware load test

Hierarchical to: No other components

FPT_TST_CIMC.3.1 A cryptographic mechanism using a FIPS-approved or recommended authentication technique (e.g., an authentication code, keyed hash, or digital signature algorithm) shall be applied to all security-relevant software and firmware that can be externally loaded into the TOE.

FPT_TST_CIMC.3.2 The TSF shall verify the authentication code, keyed hash, or digital signature whenever the software or firmware is externally loaded into the TOE. If verification fails, the TSF shall [ST assignment: *action to be taken*].

Application Note: The ST should specify the action to be taken if the signature verification fails.

Dependencies: FPT_AMT.1 Abstract Machine Testing

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria. It satisfies the security objective O.Integrity protection of user data and software and O.Periodically check integrity.

6.9 Certificate Profile Management (Mandatory)

A certificate profile defines the set of acceptable values for fields and extensions in a certificate. Examples of information that may be specified in a certificate profile include:

- constraints on the key owner's identifier (e.g., subject and/or subjectAltName in X.509);
- the set of allowable algorithms for the subject's public/private key pair;
- the certificate issuer's identifier (e.g., issuer and/or issuerAltName in X.509);
- the limitations on the length of time for which the certificate is valid;
- additional information that may/must be included in a certificate (e.g., which extensions may/must be included in an X.509 certificate);
- whether the subject of the certificate may be a CA;
- the types of operations that may be performed using the private key corresponding to the public key in the certificate (e.g., possible values for keyUsage and/or extKeyUsage in X.509);
- the policy (policies) under which the certificate may/must be issued.

There are two sets of requirements for Certificate Profile Management, Security Level 1 requirements and Security Levels 2, 3, and 4 requirements.

SECURITY LEVEL 1

FMT_MOF_CIMC.2 Certificate profile management

Hierarchical to: No other components.

FMT_MOF_CIMC.2.1 The TOE shall implement a certificate profile and shall ensure that issued certificates are consistent with that profile.

FMT_MOF_CIMC.2.2 The TOE shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

- the key owner's identifier;
- the algorithm identifier for the subject's public/private key pair;
- the identifier of the certificate issuer;

- the length of time for which the certificate is valid;

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.Configuration management.

SECURITY LEVELS 2, 3, AND 4

FMT_MOF_CIMC.3 Extended certificate profile management

Hierarchical to: FMT_MOF_CIMC.2

FMT_MOF_CIMC.3.1 The TOE shall implement a certificate profile and shall ensure that issued certificates are consistent with that profile.

FMT_MOF_CIMC.3.2 The TOE shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

- the key owner's identifier;
- the algorithm identifier for the subject's public/private key pair;
- the identifier of the certificate issuer;
- the length of time for which the certificate is valid;

FMT_MOF_CIMC.3.3 If the certificates generated are X.509 certificates, the TOE shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

- **keyUsage**;
- **basicConstraints**;
- **certificatePolicies**

FMT_MOF_CIMC.3.4 The Administrator shall specify the acceptable set of certificate extensions.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.Configuration management.

6.10 Certificate Revocation List Profile Management

A certificate revocation list profile is used to define the set of acceptable values for fields and extensions in a CRL. Examples of values that may be covered by a certificate revocation list profile include:

- **extensions** – the set of extensions that may/must be included in a CRL and the value of each extension's criticality bit.
- **issuer**, **issuerAltName** – the name of the CRL issuer.
- **nextUpdate** – the lifetime of a CRL.

There are two sets of requirements for Certificate Revocation List Profile Management, Security Level 1 requirements and Security Levels 2, 3, and 4 requirements.

SECURITY LEVEL 1

FMT_MOF_CIMC.4 Certificate revocation list profile management

Hierarchical to: No other components.

FMT_MOF_CIMC.4.1 If a CIMC issues CRLs, the TOE must implement a certificate revocation list profile and ensure that issued CRLs are consistent with the certificate revocation list profile.

FMT_MOF_CIMC.4.2 TOEs that issue CRLs shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

- **issuer;**
- **issuerAltName** (NOTE: If a CIMC does not issue CRLs with this extension, then it is not required within the certificate revocation list profile.)

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.Configuration management.

SECURITY LEVELS 2, 3, AND 4

FMT_MOF_CIMC.5 Extended certificate revocation list profile management

Hierarchical to: FMT_MOF_CIMC.4

FMT_MOF_CIMC.5.1 If a CIMC issues CRLs, the TOE must implement a certificate revocation list profile and ensure that issued CRLs are consistent with the certificate revocation list profile.

FMT_MOF_CIMC.5.2 TOEs that issue CRLs shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

- **issuer;**
- **issuerAltName** (NOTE: If a CIMC does not issue CRLs with this extension, then it is not required within the certificate revocation list profile.)
- **nextUpdate** (i.e., lifetime of a CRL).

FMT_MOF_CIMC.5.3 The Administrator shall specify the acceptable set of CRL and CRL entry extensions.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.Configuration management.

6.11 Online Certificate Status Protocol (OCSP) Profile Management

An online certificate status protocol profile is used to define the set of acceptable values for the fields in an OCSP response. The OCSP profile may specify the type(s) of responses that the CIMC may generate (i.e., acceptable values for **responseType**) as well as the set of acceptable values for the fields within the acceptable response types. Examples of values that may be covered by an OCSP profile for the basic response type include:

- **ResponderID** - the identifier of the OCSP responder
- **nextUpdate** – limitations on the lifetime of an OCSP response

FMT_MOF_CIMC.6 OCSP profile management

Hierarchical to: No other components.

FMT_MOF_CIMC.6.1 If a CIMC issues OCSP responses, the TOE must implement an OCSP profile and ensure that issued OCSP responses are consistent with the OCSP profile.

FMT_MOF_CIMC.6.2 TOEs that issue OCSP responses shall require the Administrator to specify the set of acceptable values for the **responseType** field (unless the CIMC can only issue responses of the basic response type).

FMT_MOF_CIMC.6.3 If the TOE is configured to allow OCSP responses of the basic response type, the TOE shall require the Administrator to specify the set of acceptable values for the following fields within the basic response type:

- **ResponderID** - the identifier of the OCSP responder
- **nextUpdate** – limitations on the lifetime of an OCSP response

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. It supports the security objective O.Configuration management.

6.12 Certificate Registration (Mandatory)

The functions in this section address the validation, approval, and signing of public key certificates.

X.509 public key certificates issued by CIMCs must be compliant with the X.509 standard. Any fields or extensions to be included in an X.509 certificate will either be created by the CIMC according to the rules of the X.509 standard or validated by the CIMC to ensure compliance.

The data entered in each field and extension to be included in a certificate must be approved. Generally, a certificate field or extension value may be approved in one of four ways:

1. The data may be approved manually by an Officer.
2. An automated process may be used to review and approve the data.
3. The value for a field or extension may be automatically generated by the CIMC.
4. The value for a field or extension may be taken from the certificate profile.

FDP_CIMC_CER.1 Certificate Generation

Hierarchical to: No other components.

FDP_CIMC_CER.1.1 The TSF shall only generate certificates that are consistent with the currently defined certificate profile.

FDP_CIMC_CER.1.2 The TSF shall verify that the prospective certificate subject possesses the private key that corresponds to the public key in the certificate request before issuing a certificate, unless the public/private key pair was generated by the TSF, whenever the private key may be used to generate digital signatures.

FDP_CIMC_CER.1.3 If the TSF generates X.509 certificates, it shall only generate certificates that comply with requirements for certificates as specified in ITU-T Recommendation X.509. At a minimum, the TSF shall ensure that:

a) The **version** field shall contain the integer **0**, **1**, or **2**.

b) If the certificate contains an **issuerUniqueID** or **subjectUniqueID** then the **version** field shall contain the integer **1** or **2**.

c) If the certificate contains **extensions** then the **version** field shall contain the integer **2**.

d) The **serialNumber** shall be unique with respect to the issuing Certification Authority.

e) The **validity** field shall specify a **notBefore** value that does not precede the current time and a **notAfter** value that does not precede the value specified in **notBefore**.

f) If the **issuer** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical **issuerAltName** extension.

g) If the **subject** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical **subjectAltName** extension.

h) The **signature** field and the **algorithm** in the **subjectPublicKeyInfo** field shall contain the OID for a FIPS-approved or recommended algorithm.

Dependencies: No dependencies.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

SECURITY LEVELS 3 and 4

In addition to the certificate generation requirements specified for Security Levels 1 and 2, FDP_CIMC_POP.1 shall apply for Security Levels 3 and 4.

FDP_CIMC_POP.1 Proof of possession for key management keys

Hierarchical to: No other components.

FDP_CIMC_POP.1.1 The TSF shall verify that the prospective certificate subject possesses the private key that corresponds to the public key in a certificate request before exporting the certificate from the TOE in plaintext form, unless the public/private key pair was generated by the TSF, whenever the private key may not be used to generate digital signatures.

FDP_CIMC_POP.1.2 If the certificate is exported from the TOE before proof of possession has been performed, then the certificate shall be encrypted in such a way that knowledge of the private key corresponding to the public key in the certificate shall be required to decrypt the certificate.

Dependencies: No dependencies.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.13 Certificate Revocation

The functions in this section address the validation and approval of certificate revocation information.

6.13.1 Certificate Revocation List Validation

Certificate revocation lists (CRLs) issued by CIMCs shall be compliant with the X.509 standard. Any fields or extensions to be included in a CRL shall be created by the CIMC according to the X.509 standard.

FDP_CIMC_CRL.1 Certificate revocation list validation

Hierarchical to: No other components.

FDP_CIMC_CRL.1.1 The CIMC shall verify that all mandatory fields in the CRL contain values in accordance with ITU-T Recommendation X.509. At a minimum, the following items shall be validated:

1. If the **version** field is present, then it shall contain a **1**.
2. If the CRL contains any critical extensions, then the **version** field shall be present and contain the integer **1**.
3. If the **issuer** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the CRL shall contain a critical **issuerAltName** extension.
4. The **signature** and **signatureAlgorithm** fields shall contain the OID for a FIPS-approved digital signature algorithm.
5. The **thisUpdate** field shall indicate the issue date of the CRL.
6. The time specified in the **nextUpdate** field (if populated) shall not precede the time specified in the **thisUpdate** field.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.13.2 OCSP Basic Response Validation

OCSP basic responses issued by CIMCs shall be compliant with IETF RFC 2560. Any fields or extensions to be included in an OCSP response shall be created by the CIMC according to IETF RFC 2560.

FDP_CIMC_OCSP.1 OCSP basic response validation

Hierarchical to: No other components.

FDP_CIMC_OCSP.1.1 The CIMC shall verify that all mandatory fields in the OCSP basic response contain values in accordance with IETF RFC 2560. At a minimum, the following items shall be validated:

1. The **version** field shall contain a **0**.
2. If the **issuer** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the response shall contain a critical **issuerAltName** extension.
3. The **signatureAlgorithm** field shall contain the OID for a FIPS-approved digital signature algorithm.
4. The **thisUpdate** field shall indicate the time at which the status being indicated is known to be correct.
5. The **producedAt** field shall indicate the time at which the OCSP responder signed the response.
6. The time specified in the **nextUpdate** field (if populated) shall not precede the time specified in the **thisUpdate** field.

Dependencies: No dependencies

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the Common Criteria.

6.14 Cryptographic Modules

In many cases, a CIMC may use a single cryptographic module to perform all cryptographic functions. However performance and cost considerations may require a design that uses several separate cryptographic modules performing distinct functions. For example, a level 3 CIMC might use a hardware

cryptographic module validated to FIPS 140 level 3 to sign certificates and CRLs, but use a software cryptographic module that has only been validated to level 2 to compute authentication codes for general transaction messages.

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [assignment: *encryption, decryption, random number generation, signature generation, signature verification, authentication code generation, authentication code verification, hash generation, hash verification, keyed-hash message authentication code generation, keyed-hash message authentication code verification*] in accordance with a specified FIPS-approved or recommended algorithm that meets a FIPS standard.

Application Note: The ST should specify the cryptographic operations that are being performed.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

In Section 6.16 below, cryptographic functions and keys are categorized based on their uses within a CIMC. Security requirements are then imposed on the cryptographic modules within a CIMC based on the Security Level of the CIMC, the types of cryptographic functions that are performed by the cryptographic module, and the types of keys that are stored within the cryptographic module.

6.15 Strength of Function

6.15.1 Authentication Mechanisms

The authentication mechanisms specified in FIA_UAU.1 shall meet the following strength of function requirements:

1. For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods.)
2. For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.

6.15.2 Cryptographic Modules

FIPS 140 validated cryptographic modules must perform all cryptographic functions performed by CIMCs. FIPS 140 validated cryptographic modules are also required to generate cryptographic keys and to store plaintext private and secret keys.

6.15.2.1 Encryption and FIPS 140 Validated Modules

As noted earlier in the document, references to FIPS 140 refer to the most recent version of the standard and the most recent version can be found at http://csrc.nist.gov/cryptval.

6.15.2.1.1 Encryption Algorithms

The encryption specified for:

FAU_STG.1	Protected audit trail storage
FCO_NRO_CIMC.4	Advanced verification of origin
FDP_ACF_CIMC.2	User private key confidentiality protection
FDP_ACF_CIMC.3	User secret key confidentiality protection
FDP_CIMC_BKP.2	Extended CIMC backup and recovery
FDP_ETC_CIMC.4	User private and secret key export
FDP_ETC_CIMC.5	Extended user private and secret key export
FDP_SDI_CIMC.3	Stored public key integrity monitoring and action
FMT_MTD_CIMC.4	TSF private key confidentiality protection
FMT_MTD_CIMC.5	TSF secret key confidentiality protection
FMT_MTD_CIMC.6	TSF private and secret key export
FMT_MTD_CIMC.7	Extended TSF private and secret key export
FPT_CIMC_TSP.1	Audit log signing event
FPT_CIMC_TSP.2	Audit log time stamp event
FPT_TST_CIMC.2	Software/firmware integrity test
FPT_TST_CIMC.3	Software/firmware load test

shall be performed using a FIPS-approved or recommended algorithm.

6.15.2.1.2 FIPS 140 Validated Cryptographic Modules

Cryptographic modules specified for:

FCS_CKM.1	Cryptographic key generation
FDP_ACF_CIMC.2	User private key confidentiality protection
FDP_ACF_CIMC.3	User secret key confidentiality protection
FDP_ETC_CIMC.4	User private and secret key export
FDP_ETC_CIMC.5	Extended user private and secret key export
FDP_SDI_CIMC.3	Stored public key integrity monitoring and action
FMT_MTD_CIMC.4	TSF private key confidentiality protection
FMT_MTD_CIMC.5	TSF secret key confidentiality protection
FMT_MTD_CIMC.6	TSF private and secret key export
FMT_MTD_CIMC.7	Extended TSF private and secret key export
FPT_CIMC_TSP.1	Audit log signing event

shall be validated against FIPS 140.

6.15.2.1.3 Split Knowledge Procedures

Split-knowledge procedures specified in:

FDP_ETC_CIMC.4	User private and secret key export
FDP_ETC_CIMC.5	Extended user private and secret key export
FMT_MTD_CIMC.6	TSF private and secret key export
FMT_MTD_CIMC.7	Extended TSF private and secret key export

shall be implemented and validated as specified in FIPS 140.

6.15.2.1.4 Authentication Codes

The authentication code specified in:

FAU_STG.1	Protected audit trail storage
FCO_NRO_CIMC.4	Advanced verification of origin

FDP_CIMC_BKP.2	Extended CIMC backup and recovery
FDP_CIMC_TSP.1	Audit log signing event
FDP_SDI_CIMC.3	Stored public key integrity monitoring and action
FPT_TST_CIMC.2	Software/firmware integrity test
FPT_TST_CIMC.3	Software/firmware load test

shall be a FIPS-approved or recommended authentication code.

All cryptographic operations performed by the TOE shall be performed in a FIPS 140 validated cryptographic module operating in a FIPS-approved or recommended mode of operation.

Table 6 specifies for each category of use for a private or secret key and CIMC Security Level, the required overall FIPS 140 level for the validated cryptographic module.

Table 6. FIPS 140 Security Level for Validated Cryptographic Module

Required Overall FIPS 140 Level for CIMC Cryptographic Modules				
Category of Use	**CIMC Security Level 1**	**CIMC Security Level 2**	**CIMC Security Level 3**	**CIMC Security Level 4**
Certificate and Status Signing				
- single party signature	1	2	3	4
- multiparty signature	1	1	2	3
Integrity or Approval Authentication				
- single approval	1	2	2	3
- dual approval	1	1	2	2
General Authentication	1	1	2	2
Long Term Private Key Protection	1	2	3	4
Long Term Confidentiality	1	1	2	2
Short Term Private key Protection	1	1	2	2
Short Term Confidentiality	1	1	1	2

The Security Level of the validated cryptographic module will be selected from the above table using the CIMC level (column) and the category of use (row). For example, if the CIMC level is 2 and the key is used for general authentication, the cryptographic module must be validated to FIPS 140 Security Level 1.

6.15.2.2 Cryptographic Functions That Do Not Involve Private or Secret Keys

There are two other cryptographic functions that may be performed in CIMCs that do not require private or secret keys. These include:

1. *Hash Generation*: One-way hash functions may be used in the process of signature generation and verification (a signature is typically generated by applying a private key to the hash of the message). The generation of a hash does not require a key. Therefore, hash generation does not have the same confidentiality requirements of other cryptographic functions.
2. *Signature Verification*: Signatures are verified from a message text and a public key.

For a cryptographic module that only performs signature verification and/or keyless hash generation functions, the overall required FIPS 140 Security Level shall be Security Level 1 for CIMC Levels 1 through 3 and Security Level 2 for CIMC Level 4.

7 TOE SECURITY ASSURANCE REQUIREMENTS

This section specifies the assurance requirements for CIMCs. Details of the assurance components specified in this section may be found in part 3 of the Common Criteria.

7.1.1 Security Level 1 Security Assurance

The assurance requirements for CIMCs at Security Level 1 are the requirements for EAL1 with the addition of ATE_FUN.1 Functional Testing and AVA_SOF.1 Strength of TOE Security Function Evaluation. These requirements are designed to provide evidence that the CIMC functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.

The assurance requirements for Security Level 1 are summarized below.

Table 7. Security Level 1 Assurance Requirements

Assurance Class	Component ID	Component Title	EAL Level
Configuration Management	ACM_CAP.1	Version numbers	EAL1
Delivery and Operation	ADO_IGS.1	Installation, generation, and start-up procedures	EAL1 - 7
Development	ADV_FSP.1	Informal functional specification	EAL1 - 3
	ADV_RCR.1	Informal correspondence demonstration	EAL1 - 4
Guidance Documents	AGD_ADM.1	Administrator guidance	EAL1 - 7
	AGD_USR.1	User guidance	EAL1 - 7
Tests	ATE_FUN.1	Functional testing	EAL2 - 5
	ATE_IND.1	Independent testing – conformance	EAL1
Vulnerability Assessment	AVA_SOF.1	Strength of TOE security function evaluation	EAL2 - 7

7.1.2 Security Level 2 Security Assurance

The assurance requirements for CIMCs at Security Level 2 are those specified in *CSPP - Guidance for COTS Security Protection Profiles*.[3] The CSPP assurance level would be EAL3 except for ADV_HLD.2 Descriptive high-level design. The following EAL4 assurance requirements are also required for this assurance level: ACM_SCP.2 Problem tracking configuration management coverage, ADV_SPM.1 Informal TOE security policy model, ALC_FLR.2 Flaw reporting procedures, and AVA_MSU.2 Validation of analysis components that are at the EAL4 level. The assurance requirements of CSPP stress assurance through vendor actions that are currently within best commercial practices. The assurance requirements of CSPP, which shall be referred to as EAL-CSPP, stress assurance through vendor actions that are within the bounds of current best commercial practice. EAL-CSPP provides, primarily via review of vendor supplied evidence, independent confirmation that these actions have been competently performed. EAL-CSPP also includes the following independent, third-party analysis: (1) confirmation of system generation and installation procedures, (2) verification that the system security state is not misrepresented, (3) verification of a sample of the vendor functional testing, (4) searching for obvious vulnerabilities, and (5) independent functional testing.

The assurance requirements for EAL-CSPP are summarized below.

Table 8. Security Level 2 Assurance Requirements

Assurance Class	Component ID	Component Title	EAL Level

[3] Version 1.0 of *CSPP - Guidance for COTS Security Protection Profiles* (NISTIR 6462) may be obtained from http://csrc.nist.gov/cc/pp/pplist.htm#CSPP.

Table 8. Security Level 2 Assurance Requirements

Assurance Class	Component ID	Component Title	EAL Level
Configuration Management	ACM_CAP.3	Authorization controls	EAL3
	ACM_SCP.2	Problem tracking CM coverage	EAL4
Delivery and Operation	ADO_DEL.1	Delivery procedures	EAL2 - 3
	ADO_IGS.1	Installation, generation, and start-up procedures	EAL1 – 7
Development	ADV_FSP.1	Informal functional specification	EAL1 - 3
	ADV_HLD.1	Descriptive high-level design	EAL2
	ADV_RCR.1	Informal correspondence demonstration	EAL1 – 4
	ADV_SPM.1	Informal TOE security policy model	EAL4
Guidance Documents	AGD_ADM.1	Administrator guidance	EAL1 – 7
	AGD_USR.1	User guidance	EAL1 - 7
Life Cycle Support	ALC_DVS.1	Identification of security measures	EAL3 - 5
	ALC_FLR.2	Flaw reporting procedures	None
Tests	ATE_COV.2	Analysis of coverage	EAL3 – 5
	ATE_DPT.1	Testing - high-level design	EAL3 – 4
	ATE_FUN.1	Functional testing	EAL2 – 5
	ATE_IND.2	Independent testing - sample	EAL2 – 6
Vulnerability Assessment	AVA_MSU.2	Validation of analysis	EAL4 – 5
	AVA_SOF.1	Strength of TOE security function evaluation	EAL2 – 7
	AVA_VLA.1	Developer vulnerability analysis	EAL2 - 3

7.1.3 Security Level 3 Security Assurance

The assurance requirements for CIMCs at Security Level 3 are extracted from EAL Levels 3 and 4, with the addition of ALC_FLR.2: Flaw reporting procedures. CIMC Security Level 3 includes all of requirements from CC EAL3, augmenting many of the EAL3 requirements. Of the 22 CIMC Security Level 3 requirements, 12 are from EAL3, 9 are from EAL4, and one (ALC_FLR.2) does not appear in any of the EAL levels.

Table 9. Security Level 3 Assurance Requirements

Assurance Class	Component ID	Component Title	EAL Level
Configuration Management	ACM_CAP.3	Authorization controls	EAL3
	ACM_SCP.2	Problem tracking CM coverage	EAL4
Delivery and Operation	ADO_DEL.2	Detection of modification	EAL4 – 6
	ADO_IGS.1	Installation, generation, and start-up procedures	EAL1 – 7
Development	ADV_FSP.2	Fully defined external interfaces	EAL4
	ADV_HLD.2	Security enforcing high-level design	EAL3 – 4
	ADV_IMP.1	Subset of the implementation of the TSF	EAL4
	ADV_LLD.1	Descriptive low-level design	EAL4 – 5
	ADV_RCR.1	Informal correspondence demonstration	EAL1 – 4

Table 9. Security Level 3 Assurance Requirements

Assurance Class	Component ID	Component Title	EAL Level
	ADV_SPM.1	Informal TOE security policy model	EAL4
Guidance Documents	AGD_ADM.1	Administrator guidance	EAL1 – 7
	AGD_USR.1	User guidance	EAL1 – 7
Life Cycle Support	ALC_DVS.1	Identification of security measures	EAL3 – 5
	ALC_FLR.2	Flaw reporting procedures	None
	ALC_TAT.1	Well-defined development tools	EAL4
Tests	ATE_COV.2	Analysis of coverage	EAL3 – 5
	ATE_DPT.1	Testing: high-level design	EAL3 – 4
	ATE_FUN.1	Functional testing	EAL2 – 5
	ATE_IND.2	Independent testing - sample	EAL2 – 6
Vulnerability Assessment	AVA_MSU.2	Validation of analysis	EAL4 - 5
	AVA_SOF.1	Strength of TOE security function evaluation	EAL2 - 7
	AVA_VLA.2	Independent vulnerability analysis	EAL4

7.1.4 Security Level 4 Security Assurance

The assurance requirements for CIMCs at Security Level 4 are extracted from EAL Levels 4 and 5, with the addition of ALC_FLR.3: Systematic flaw remediation. Of the 25 requirements, 21 are from EAL4, 3 are from EAL5, and one (ALC_FLR.3) does not appear in any of the EAL levels.

Table 10. Security Level 4 Assurance Requirements

Assurance Class	Component ID	Component Title	EAL Level
Configuration Management	ACM_AUT.1	Partial CM automation	EAL4 – 5
	ACM_CAP.4	Generation support and acceptance procedures	EAL4 – 5
	ACM_SCP.2	Problem tracking CM coverage	EAL4
Delivery and Operation	ADO_DEL.2	Detection of modification	EAL4 - 6
	ADO_IGS.1	Installation, generation, and start-up procedures	EAL1 – 7
Development	ADV_FSP.2	Fully defined external interfaces	EAL4
	ADV_HLD.2	Security enforcing high-level design	EAL3 - 4
	ADV_IMP.1	Subset of the implementation of the TSF	EAL4
	ADV_INT.1	Modularity	EAL5
	ADV_LLD.1	Descriptive low-level design	EAL4 – 5
	ADV_RCR.1	Informal correspondence demonstration	EAL1 - 4
	ADV_SPM.1	Informal TOE security policy model	EAL4
Guidance Documents	AGD_ADM.1	Administrator guidance	EAL1 – 7
	AGD_USR.1	User guidance	EAL1 – 7
Life Cycle Support	ALC_DVS.1	Identification of security measures	EAL3 – 5
	ALC_FLR.3	Systematic flaw remediation	None
	ALC_LCD.1	Developer defined life-cycle model	EAL4

Table 10. Security Level 4 Assurance Requirements

Assurance Class	Component ID	Component Title	EAL Level
	ALC_TAT.1	Well-defined development tools	EAL4
Tests	ATE_COV.2	Analysis of coverage	EAL3 – 5
	ATE_DPT.2	Testing: low-level design	EAL5 – 6
	ATE_FUN.1	Functional testing	EAL2 – 5
	ATE_IND.2	Independent testing - sample	EAL2 – 6
Vulnerability Assessment	AVA_MSU.2	Validation of analysis	EAL4 – 5
	AVA_SOF.1	Strength of TOE security function evaluation	EAL2 – 7
	AVA_VLA.3	Moderately resistant	EAL5

8 RATIONALE

This section includes the rationale for the functional and assurance requirements specified for the TOE. The rationale is based on specified objectives, threats, assumptions, and policies.

8.1 Security Objectives Rationale

This section demonstrates that the stated security objectives counter all identified threats, policies, or assumptions.

8.2 Security Objectives Coverage

The following tables provide a mapping of security objectives to the environment defined by the threats, policies, and assumptions, illustrating that each security objective covers at least one threat, policy or assumption and that each threat, policy or assumption is covered by at least one security objective.

Table 11. IT Security Objectives Related to Threats

IT Security Objective	Threat
O.Administrators, Operators, Officers and Auditors guidance documentation	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions, T.Disclosure of private and secret keys
O.Certificates	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Configuration management	T.Critical system component fails, T.Malicious code exploitation, T.TOE developed with inadequate TSF self protection

Table 11. IT Security Objectives Related to Threats

IT Security Objective	Threat
O.Control unknown source communication traffic	T.Hacker gains access
O.Cryptographic functions	T.Disclosure of private and secret keys, T.Modification of secret/private keys
O.Data import/export	T.Message content modification, T.User abuses authorization to collect and/or send data
O.Detect modifications of firmware, software, and backup data	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions, T.User error makes data inaccessible
O.Examine source code for developer flaws	T.Flawed code
O.General user documentation	T.Social engineering
O.Individual accountability and audit records	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions, T.Administrative errors of omission, T.Hacker gains access, T.User abuses authorization to collect and/or send data
O.Integrity protection of user data and software	T. Malicious code exploitation, T.Modification of private/secret keys
O.Lifecycle security	T.Critical system component fails, T. Malicious code exploitation, T.Social engineering
O.Limitation of administrative access control	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions, T.Disclosure of secret and private keys
O.Maintain user attributes	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions

Table 11. IT Security Objectives Related to Threats

IT Security Objective	Threat
O.Manage behavior of security functions	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions, T.Critical system component fails
O.Non-repudiation	T.Sender denies sending information
O.Object and data recovery free from malicious code	T.Malicious code exploitation, T.Modification of secret/private keys
O.Periodically check integrity	T.Malicious code exploitation
O.Preservation/trusted recovery of secure state	T.Critical system component fails
O.Procedures for preventing malicious code	T.Social engineering
O.Protect stored audit records	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions, T.Modification of secret/private keys
O.Protect user and TSF data during internal transfer	T.Flawed code, T.User abuses authorization to collect and/or send data
O.React to detected attacks	T.Hacker gains access
O.Repair identified security flaws	T.Flawed code, T.Critical system component fails
O.Require inspection for downloads	T.Malicious code exploitation
O.Respond to possible loss of stored audit records	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Restrict actions before authentication	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Security roles	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Security-relevant configuration management	T.Administrative errors of omission
O.Sufficient backup storage and effective restoration	T.Critical system component fails

Table 11. IT Security Objectives Related to Threats

IT Security Objective	Threat
O.Time stamps	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions, T.Critical system component fails
O.Trusted path	T.Hacker gains access, T.Message content modification, T.User abuses authorization to collect and/or send data
O.User authorization management	T.Administrative errors of omission
O.Validation of security function	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions, T.Malicious code exploitation

Table 12. Non-IT Security Objectives Rationale

Non-IT Security Objective	Threat
O.Administrative Training	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.CPS	T.Administrative errors of omission
O.Credentials	T.Disclosure of private and secret keys
O.Installation	T.Critical system component fails
O.Notify authorities of security issues	T.Hacker gains access
O.Operating System	T.Flawed code
O.Physical Protection	T.Hacker physical access

Table 13. Organizational Security Policies Related to Security Objectives

Security Policy	Objective
P.Authorized use of information	O.Auditors review audit logs O.Maintain user attributes

	O.Restrict actions before authentication O.Security roles O.User authorization management
P.Cryptography	O.Cryptographic functions

Table 14. Assumptions Related to IT Security Objectives

Assumption	IT Security Objective
A.Auditors Review Audit Logs	O.Auditors Review Audit Logs
A.Authentication Data Management	O.Authentication Data Management
A.Communications Protection	O.Communications Protection
A.Competent Administrators, Operators, Officers and Auditors	O.Competent Administrators, Operators, Officers and Auditors
A.Cooperative Users	O.Cooperative Users
A.Disposal of Authentication Data	O.Disposal of Authentication Data
A.Hardware Integrity	O.Hardware Integrity
A.Malicious Code Not Signed	O.Malicious Code Not Signed
A.No Abusive Administrators, Operators, Officers and Auditors	O.No Abusive Administrators, Operators, Officers and Auditors
A.Physical Protection	O.Physical Protection
A.Operating System	O.Operating System
A.Social Engineering Training	O.Social Engineering Training

8.2.1 Security Objectives Sufficiency

The following discussions provide information regarding:

1. Why the identified security objectives provide for effective countermeasures to the threats;

2. Why the identified security objectives provide complete coverage of each organizational security policy;

3. Why the identified security objectives uphold each assumption.

8.2.1.1 Threats and Objectives Sufficiency

T.Administrative errors of omission addresses errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application. It is countered by:

> **O.CPS** provides administrators, operators, officers, and auditors with information regarding the policies and practices used by the system.
>
> **O.Individual accountability and audit records** provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms.
>
> **O.Security-relevant configuration management** ensures that system security policy data and enforcement functions, and other security-relevant configuration data are managed and updated. This ensures that they are consistent with organizational security policies.
>
> **O.User authorization management** ensures that user authorization and privilege data are managed and updated. This ensures that they are consistent with organizational security and personnel policies.

T.Administrators, Operators, Officers and Auditors commit errors or hostile actions addresses:

- Errors committed by administrative personnel that directly compromise organizational security objectives, change the technical security policy enforced by the system or application, or
- Malicious obstruction by administrative personnel of organizational security objectives or modification of the system's configuration to allow security violations to occur.

It is countered by:

> **O. Administrative Training** ensures that users receive training in performing effective security practices.
>
> **O.Administrators, Operators, Officers and Auditors guidance documentation** which deters administrative personnel errors by providing adequate guidance.
>
> **O.Certificates** ensures that certificates, certificate revocation lists, and certificate status information are valid.
>
> **O.Detect modifications of firmware, software, and backup data of backup hardware, firmware, and software** ensures that if the backup components have been modified, that it is detected.
>
> **O.Individual accountability and audit records** provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms.
>
> **O.Limitation of administrative access control**. The administrative functions are designed in such a way that administrative personnel do not automatically have access to user objects, except for necessary exceptions. In general, the exceptions tend to be role specific.

O.Maintain user attributes. Maintains a set of security attributes (which may include group membership, access rights, etc.) associated with individual users in addition to user identity.

O.Manage behavior of security functions provides management controls/functions for security mechanisms.

O.Protect stored audit records ensures that audit records are protected against unauthorized access, modification, or deletion to provide for traceability of user actions.

O.Respond to possible loss of stored audit records ensures that only auditable events executed by the Auditor shall be audited if the audit trail is full.

O.Restrict actions before authentication ensures that only a limited set of actions may be performed before a user is authenticated.

O.Security roles ensures that security-relevant roles are specified and that users are assigned to one (or more) of the defined roles.

O.Time stamps ensures that time stamps are provided to verify a sequence of events.

O.Validation of security function. Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures such as underlying machine testing and integrity checks.

T.Critical system component fails addresses the failure of one or more system components that results in the loss of system-critical functionality. This threat is relevant when there are components that may fail due to hardware and/or software imperfections and the availability of system functionality is important.

It is countered by:

O.Configuration management assures that a configuration management program is implemented. The configuration management program includes configuration identification and change control.

O.Installation ensures that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.

O.Lifecycle security provides tools and techniques that are used throughout the development phase. O. Lifecycle security also addresses the detection and resolution of flaws discovered during the operational phase.

O.Manage behavior of security functions provides management controls/functions for security mechanisms.

O.Preservation/trusted recovery of secure state ensures that the system will continue some form of operation in the presence of failures. Also, this objective is relevant when system failures could result in insecure states that, when the system returns to operational mode (or continues to operate), could lead to security compromises.

O.Repair identified security flaws. The vendor repairs security flaws that have been identified by a user.

O.Sufficient backup storage and effective restoration ensures that there is sufficient backup storage and effective restoration to recreate the system, when required.

O.Time stamps provides time stamps to ensure that the sequencing of events can be verified.

T.Disclosure of private and secret keys addresses the unauthorized disclosure of secret and/or private keys.

It is countered by:

> **O.Administrators, Operators, Officers and Auditors guidance documentation** ensures that adequate documentation on securely configuring and operating the CIMC is available to Administrators, Operators, Officers and Auditors. This documentation will minimize errors committed by those users.
>
> **O.Credentials** ensures that all access credentials are protected by the users in a manner that maintains IT security.
>
> **O.Cryptographic functions** ensures that TOE implements approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and uses validated cryptographic modules.
>
> **O.Limitation of administrative access control**. The administrative functions are designed in such a way that administrative personnel do not automatically have access to user objects, except for necessary exceptions. In general, the exceptions tend to be role specific.

T.Flawed code addresses accidental or deliberate flaws in code made by the developer. Examples of accidental flaws are lack of engineering detail or bad design. An example of a deliberate flaw would be the inclusion of a trapdoor for later entry into the TOE.

It is countered by:

> **O.Examine source code for developer flaws** ensures that the source code is examined after the TOE has been installed.
>
> **O.Operating System** ensures that the operating system meets security requirements recommended by the National Institute of Standards and Technology.
>
> **O.Protect user and TSF data during internal transfer** ensures the integrity of user and TSF data transferred internally within the TOE.
>
> **O.Repair identified security flaws** ensures that the vendor repairs security flaws that have been identified by a user.

T.Hacker gains access addresses:

- Weak system access control mechanisms or user attributes
- Weak implementation methods of the system access control
- Vulnerabilities found in system or application code that allow a hacker to break into a system undetected.

It is countered by:

> **O.Control unknown source communication traffic** ensures that communication traffic from an unknown source is controlled (e.g., rerouted or discarded) to prevent potential damage. Various kinds of hacker attacks can be detected or prevented by rerouting or discarding suspected hacker traffic.

O.Individual accountability and audit records provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms.

O.Notify authorities of security issues ensures that proper authorities are notified regarding any security issues that impact their systems. This minimizes the potential for the loss or compromise of data.

O.React to detected attacks ensures that automated notification or other reactions to the TSF-discovered attacks is implemented in an effort to identify attacks and to create an attack deterrent. This objective is relevant if actions that the organization deems essential also pose a potential attack that could be exploited.

O.Trusted path ensures that a trusted path is established between the user and the system. Execution of a user-requested action must be made via a trusted path with the following properties:

- The path is logically distinct from, and cannot be confused with other communication paths (by either the user or the system) and
- The path provides assured identification of its end points.

The trusted-path objective is used for all trusted communication between the user and the TSF.

T.Hacker physical access addresses the threat where an individual exploits physical security weaknesses to gain physical control of system components.

It is countered by:

O.Physical Protection ensures that physical access controls are sufficient to thwart a physical attack on system components.

T.Malicious code exploitation addresses the threat where an authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets. The execution of malicious code is done through a triggering event

It is countered by:

O.Configuration management assures that a configuration management program is implemented. The configuration management program includes configuration identification and change control.

O.Integrity protection of user data and software that ensures that appropriate integrity protection is provided for user data and software.

O.Lifecycle security provides tools and techniques that are used throughout the development phase. O. Lifecycle security also addresses the detection and resolution of flaws discovered during the operational phase.

O.Object and data recovery free from malicious code ensures that the system recovers to a viable state after malicious code has been introduced and damage has occurred. The malicious code, e.g., virus or worm, is removed as part of the process.

O.Periodically check integrity ensures that periodic integrity checks are performed on both system and user data.

O.Require inspection for downloads ensures that software that is downloaded/transferred is inspected prior to being made operational.

O.Validation of security function. Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures such as underlying machine testing and integrity checks.

T.Message content modification addresses the situation where a hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient. Several kinds of modification are possible: modification of a single message, deletion or reordering of selected messages, insertion of bogus messages, replay of previous messages, and modification of accompanying message security attributes.

It is countered by:

O.Data Import/Export protects data from being sent to erroneous places and more places external to the system than allowed by the organization's security policy. Also, the import of data into the system is protected from illicit information or information not allowed by the organization's security policy.

This objective is relevant in the following scenarios:

1. When a user has the ability to give out information that could cause an outsider to send data that is not deemed acceptable by the organization's policy or from a location unacceptable by the organization's policy (e.g. adult only web sites).

2. When a user has the ability to send data to inappropriate locations or to more locations than the organization's policy allows.

3. When a hacker can flood the system (TOE) with illicit data.

O.Trusted path ensures that a trusted path is established between the user and the system. Execution of a user-requested action must be made via a trusted path with the following properties:

- The path is logically distinct from, and cannot be confused with other communication paths (by either the user or the system) and
- The path provides assured identification of its end points.

The trusted-path objective is used for all trusted communication between the user and the TSF.

T.Modification of private/secret keys addresses the unauthorized revision of a secret and/or private key.

It is countered by:

O.Cryptographic functions ensures that TOE implements approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and uses validated cryptographic modules.

O.Integrity protection of user data and software that ensures that appropriate integrity protection is provided for user data and software.

O.Object and data recovery free from malicious code ensures that the system recovers to a viable state after malicious code has been introduced and damage has occurred. The malicious code, e.g., virus or worm, is removed as part of the process.

O.Protect stored audit records ensures that audit records are protected against unauthorized access, modification, or deletion to provide for traceability of user actions.

T.Sender denies sending information addresses the situation where the sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.

It is countered by:

O.Non-repudiation which ensures that the sender/originator of a message cannot successfully deny sending the message to the recipient.

T.TOE developed with inadequate TSF self protection addresses the situation where the system or applications developer delivers code that includes security flaws that prevent the TSF from adequately protecting itself. The security flaws may be either deliberate or accidental.

It is countered by:

O.Configuration management, which assures that a configuration management program, is implemented. The configuration management program includes configuration identification and change control.

T.Social Engineering addresses the situation where a hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation

It is countered by:

O.General user documentation provides documentation for the general user and for the administrative roles. This documentation includes procedures that address potential social engineering attacks.

O.Lifecycle security provides tools and techniques that are used throughout the development phase. O. Lifecycle security also addresses the detection and resolution of flaws discovered during the operational phase.

O.Procedures for preventing malicious code provides a set of procedures and mechanisms that work to prevent incorporation of malicious code into the system.

T.User abuses authorization to collect and/or send data addresses the situation where an authorized user abuses granted authorizations by browsing files in order to collect data and/or violates export control policy by sending data to a recipient who is not authorized to receive the data.

It is countered by:

O.Data Import/Export protects data from being sent to erroneous places and more places external to the system than allowed by the organization's security policy. Also, the import of data into the system is protected from illicit information or information not allowed by the organization's security policy.

This objective is relevant in the following scenarios:

1. When a user has the ability to give out information that could cause an outsider to send data that is not deemed acceptable by the organization's policy or from a location unacceptable by the organization's policy (e.g. adult only web sites).

2. When a user has the ability to send data to inappropriate locations or to more locations than the organization's policy allows.

3. When a hacker can flood the system (TOE) with illicit data.

O.Individual accountability and audit records provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms.

O.Protect user and TSF data during internal transfer ensures the integrity of user and TSF data transferred internally within the TOE.

O.Trusted path ensures that a trusted path is established between the user and the system. Execution of a user-requested action must be made via a trusted path with the following properties:

- The path is logically distinct from, and cannot be confused with other communication paths (by either the user or the system) and
- The path provides assured identification of its end points.

The trusted-path objective is used for all trusted communication between the user and the TSF

T.User error makes data inaccessible addresses a user accidentally deleting user data. Consequently, the user data is inaccessible. Examples include the following:

- User accidentally deletes data by striking the wrong key on the keyboard or by striking the enter key as an automatic response.
- User does not understand the implications of the prompt at hand and inadvertently gives a response that deletes user data.
- User misunderstands a system command and issues a command that unintentionally deletes user data.

It is countered by:

O.Detect modifications of firmware, software, and backup data of backup hardware, firmware, and software ensures that if the backup components have been modified, that it is detected.

8.2.1.2 Policies and Objectives Sufficiency

P.Authorized use of information establishes that information is used only for its authorized purpose(s). This is addressed by the following objectives: **O.Maintain user attributes**, **O.Restrict actions before authentication**, **O.Security roles**, and **O.User authorization management**. **O.Restrict actions before authentication** ensures that the capability to perform security-relevant operations is limited to those who have been authorized to perform those operations. **O.Maintain user attributes**, **O.Security roles**, and **O.User authorization management** ensure that users are only authorized to perform those operations that are necessary to perform their jobs. Finally, **O.Auditors review audit logs** deters users from misusing the authorizations they have been provided.

P.Cryptography establishes that accepted cryptographic standards and operations shall be used in the design of the TOE. This is addressed by **O.Cryptographic functions** which ensures that such standards are used.

8.2.1.3 Assumptions and Objectives Sufficiency

A.Auditors Review Audit Logs establishes that audit logs are necessary for security-relevant events and that they must be reviewed by auditors. This is addressed by **O.Auditors Review Audit Logs**, which ensures that security-relevant events recorded in audit logs are reviewed by auditors.

A.Authentication Data Management establishes that management of user authentication data is external to the TOE. This is addressed by **O.Authentication Data Management**, which ensures that users modify their authentication data in accordance with appropriate security policy.

A.Communications Protection establishes that the communications infrastructure is outside the TOE. This is addressed by **O.Communications Protection**, which ensures that adequate physical protections are afforded the necessary communications infrastructure.

A.Competent Administrators, Operators, Officers and Auditors establishes that security of the TOE is dependent upon those that manage it. This is addressed by **O.Competent Administrators, Operators, Officers and Auditors**, which ensures that the system managers will be competent in its administration.

A.Cooperative Users establishes that a secure IT environment is required to securely operate the TOE, and that users must work within the constraints of that environment. This is addressed by **O.Cooperative Users**, which ensures that users will cooperate with the constraints established.

A.Disposal of Authentication Data establishes that users shall not retain access to the system after their authorization has been removed. This is addressed by **O.Disposal of Authentication Data**, which ensures that access to the system will be denied after a user's privileges have been removed.

A.Hardware Integrity establishes that hardware resides outside the TOE. This is addressed by **O.Hardware Integrity**, which ensures that there are hardware integrity checks to maintain a secure hardware state.

A.Malicious Code Not Signed establishes that code not designed for the TOE will not be signed by a trusted party. This is addressed by **O. Malicious Code Not Signed,** which ensures that code must be signed by a trusted party or it will not be loaded onto the system.

A.No Abusive Administrators, Operators, Officers and Auditors establishes that administrators, operators, officers, and auditors have a great deal of authority. This is addressed by **O.No Abusive Administrators, Operators, Officers and Auditors**, which ensures that individuals hired to be administrators, operators, officers, and auditors are deemed to be trustworthy.

A.Operating System establishes that an insecure operating system will compromise system security. This is addressed by **O.Operating System**, which ensures that an operating system that meets security requirements recommended by the National Institute of Standards and Technology will be used.

A.Physical Protection establishes that physical modification of the TOE hardware, software, and firmware will compromise system security. This is addressed by **O.Physical Protection**, which ensures that adequate physical protection will be provided.

A.Social Engineering establishes that individuals will attempt to gain access to the system using social engineering practices. This is addressed by **O.Social Engineering**, which ensures that all users will be training to thwart social engineering attacks.

8.3 Security Requirements Rationale

This section provides the rationale for necessity and sufficiency of security requirements, demonstrating that each of the security objectives is addressed by at least one security requirement, and that every security requirement is directed toward solving at least one objective.

8.3.1 Security Requirements Coverage

The following table provides a mapping of the relationships of security requirements to objectives, illustrating that each security requirement covers at least one objective and that each objective is covered by at least one security requirement.

Table 15. Security Functional Requirements Related to Security Objectives

Functional Requirement	Objective
FAU_GEN.1 Audit data generation	O.Individual accountability and audit records
FAU_GEN.2 User identity association	O.Individual accountability and audit records
FAU_SAR.1 Audit review	O.Individual accountability and audit records
FAU_SAR.3 Selectable audit review	O.Individual accountability and audit records
FAU_SEL.1 Selective audit	O.Individual accountability and audit records
FAU_STG.1 Protected audit trail storage	O.Protect stored audit records
FAU_STG.4 Prevention of audit data loss	O.Respond to possible loss of stored audit records
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	O.Non-repudiation, O.Control unknown source communication traffic
FCO_NRO_CIMC.4 Advanced verification of origin	O.Non-repudiation
FCS_CKM.1 Cryptographic key generation	O.Cryptographic functions
FCS_CKM.4 Cryptographic key destruction	O.React to detected attacks
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	O.React to detected attacks
FCS_COP.1 Cryptographic operation	O.Cryptographic functions
FDP_ACC.1 Subset access control	O.Limitation of administrative access control, O. Require inspections for downloads
FDP_ACF.1 Security attribute based access control	O.Limitation of administrative access
FDP_ACF_CIMC.2 User private key confidentiality protection	O.Certificates
FDP_ACF_CIMC.3 User secret key confidentiality protection	O.Certificates
FDP_CIMC_BKP.1 CIMC backup and recovery	O.Object and data recovery free from malicious code, O.Preservation/trusted recovery of secure state
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	O.Detect modifications of firmware, software, and backup data, O.Object and data recovery free from malicious code, O.Sufficient backup storage and effective restoration
FDP_CIMC_BKP.3 Advanced CIMC backup and recovery	O.Object and data recovery free from malicious code, O.Preservation/trusted recovery of secure state, O.Sufficient backup storage and effective restoration
FDP_CIMC_CER.1 Certificate Generation	O.Certificates
FDP_CIMC_CRL.1 Certificate revocation list validation	O.Certificates
FDP_CIMC_CSE.1 Certificate status export	O.Certificates
FDP_CIMC_OCSP.1 OCSP basic response validation	O.Certificates
FDP_CIMC_POP.1 Proof of possession for key management keys	O.Certificates
FDP_ETC_CIMC.4 User private and secret key export	O.Data import/export
FDP_ETC_CIMC.5 Extended user private and secret key export	O.Data import/export

Table 15. Security Functional Requirements Related to Security Objectives

Functional Requirement	Objective
FDP_ITT.1 Basic internal transfer protection	O.Integrity protection of user data and software, O.Protect user and TSF data during internal transfer
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	O.Integrity protection of user data and software
FDP_UCT.1 Basic data exchange confidentiality	O.Data import/export
FIA_AFL.1 Authentication failure handling	O.React to detected attacks
FIA_ATD.1 User attribute definition	O.Maintain user attributes
FIA_UAU.1 Timing of authentication	O.Limitation of administrative access control, O.Restrict actions before authentication
FIA_UID.1 Timing of identification	O.Individual accountability and audit records, O.Limitation of administrative access control
FIA_USB.1 User-subject binding	O.Maintain user attributes
FMT_MOF.1 Management of security functions behavior	O.Configuration management, O.Manage behavior of security functions, O.Security-relevant configuration management
FMT_MOF_CIMC.2 Certificate profile management	O.Configuration management
FMT_MOF_CIMC.3 Extended certificate profile management	O.Configuration management
FMT_MOF_CIMC.4 Certificate revocation list profile management	O.Configuration management
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	O.Configuration management
FMT_MOF_CIMC.6 OCSP Profile Management	O.Configuration management
FMT_MSA.1 Management of security attributes	O.Maintain user attributes, O.User authorization management
FMT_MSA.2 Secure security attributes	O.Security-relevant configuration management
FMT_MSA.3 Static attribute initialisation	O.Security-relevant configuration management
FMT_MTD.1 Management of TSF data	O.Individual accountability and audit records, O.Protect stored audit records
FMT_MTD_CIMC.4 TSF private key confidentiality protection	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software
FMT_MTD_CIMC.6 TSF private and secret key export	O.Data import/export
FMT_MTD_CIMC.7 Extended TSF private and secret key export	O.Data import/export
FMT_SMR.2 Restrictions on security roles	O.Security roles
FPT_AMT.1 Abstract machine testing	O.Periodically check integrity, O.Validation of security function
FPT_CIMC_TSP.1 Audit log signing event	O.Protect stored audit records
FPT_CIMC_TSP.2 Audit log time stamp event	O.Time stamps
FPT_ITC.1 Inter-TSF confidentiality during transmission	O.Data import/export
FPT_ITT.1 Basic internal TSF data transfer protection	O.Protect user and TSF data during internal transfer
FPT_STM.1 Reliable time stamps	O.Individual accountability and audit records, O.Time stamps

Table 15. Security Functional Requirements Related to Security Objectives

Functional Requirement	Objective
FPT_TST_CIMC.2 Software/firmware integrity test	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software, O.Object and data recovery free from malicious code, O.Periodically check integrity, O.Procedures for preventing malicious code, O.Validation of security function
FPT_TST_CIMC.3 Software/firmware load test	O.Integrity protection of user data and software, O.Object and data recovery free from malicious code, O.Periodically check integrity
FTP_TRP.1 Trusted path	O.Trusted path

Table 16. Security Assurance Requirements Related to Security Objectives

Assurance Requirement	Objective
ACM_AUT.1 Partial CM automation	selection of EAL3, EAL4
ACM_CAP.1 Version numbers	selection of EAL1
ACM_CAP.3 Authorization controls	selection of CSPP, EAL3
ACM_CAP.4 Generation support and acceptance procedures	selection of EAL4
ACM_SCP.2 Problem tracking CM Coverage	selection of EAL4
ADO_DEL.1 Delivery procedures	selection of CSPP
ADO_DEL.2 Detection of modification	selection of EAL4
ADO_IGS.1 Installation, Generation, and Start-up Procedures	selection of EAL1, CSPP, EAL3,EAL4
ADV_FSP.1 Informal functional specification	selection of CSPP, EAL3
ADV_FSP.2 Fully defined external interfaces	selection of EAL4
ADV_HLD.1 Descriptive High-Level Design	selection of CSPP
ADV_HLD.2 Security enforcing high-level design	selection of EAL3, EAL4
ADV_IMP.1 Subset of the implementation of the TSF	selection of EAL4
ADV_INT.1 Modularity	selection of EAL5
ADV_LLD.1 Descriptive low-level design	selection of EAL4
ADV_RCR.1 Informal Correspondence Demonstration	selection of EAL1, CSPP, EAL3, EAL4
ADV_SPM.1 Informal TOE security policy model	selection of CSPP, EAL4
AGD_ADM.1 Administrator Guidance	O.Administrators, Operators, Officers and Auditors guidance documentation, O.Procedures for preventing malicious code, selection of EAL1, CSPP, EAL3, EAL4
AGD_USR.1 User Guidance	O.Administrators, Operators,

Table 16. Security Assurance Requirements Related to Security Objectives

Assurance Requirement	Objective
	Officers and Auditors guidance documentation, O.General user documentation, O.Procedures for preventing malicious code, selection of EAL1, CSPP, EAL3, EAL4
ALC_DVS.1 Identification of security measures	selection of CSPP, EAL3, EAL4
ALC_FLR.2 Flaw reporting procedures	O.Examine source code for developer flaws, O.Lifecycle security, O.Repair identified security flaws
ALC_FLR.3 Systematic flaw remediation	O.Examine source code for developer flaws, O.Lifecycle security, O.Repair identified security flaws
ALC_LCD.1 Developer defined life-cycle model	selection of EAL4
ALC_TAT.1 Well-defined development tools	selection of EAL4
ATE_COV.2 Analysis of coverage	selection of CSPP, EAL3, EAL4
ATE_DPT.1 Testing - High-Level Design	selection of CSPP, EAL3
ATE_DPT.2 Testing: low-level design	selection of EAL5
ATE_FUN.1 Functional testing	selection of CSPP, EAL3, EAL4
ATE_IND.1 Independent Testing – Conformance	selection of EAL1
ATE_IND.2 Independent Testing - Sample	selection of CSPP, EAL3, EAL4
AVA_MSU.2 Validation of analysis	selection of CSPP, EAL3, EAL4
AVA_SOF.1 Strength of TOE Security Function Evaluation	selection of CSPP, EAL3, EAL4
AVA_VLA.1 Developer Vulnerability Analysis	selection of CSPP
AVA_VLA.2 Independent vulnerability analysis	selection of EAL4
AVA_VLA.3 Moderately resistant	selection of EAL5

8.3.2 Security Requirements Sufficiency

Authorized Users

O.Administrators, Operators, Officers and Auditors guidance documentation is provided by **AGD_ADM.1 (Administrator Guidance)** and **AGD_USR.1 (User Guidance)** which ensure that adequate guidance on the secure operation of the TOE is provided to Administrators, Operators, Officers, and Auditors.

O.Individual accountability and audit records is provided by a combination of requirements. **FIA_UID.1 (Timing of identification)** covers the requirement that users be identified before performing any security-relevant operations. **FAU_GEN.1 (Audit data generation)** and **FAU_SEL.1 (Selective**

audit) cover the requirement that security-relevant events be audited while **FAU_GEN.2 (User identity association)** and **FPT_STM.1 (Reliable time stamps)** cover the requirement that the date and time of audited events are recorded in the audit records along with the identities of the entities responsible for the actions. **FMT_MTD.1 (Management of TSF data)** covers the requirement that audit data be available for review by ensuring that users, other than Auditors, can not delete audit logs. Finally, **FAU_SAR.1 (Audit review)** and **FAU_SAR.3 (Selectable audit review)** cover the requirement that the audit records are made available for review so that individuals can be held accountable for their actions.

O.Certificates is provided by **FDP_CIMC_CER.1 (Certificate Generation)** and **FDP_CIMC_POP.1 (Proof of possession for key management keys)** which ensures that certificates are valid, and **FDP_CIMC_CRL.1 (Certificate revocation list validation)**, **FDP_CIMC_CSE.1 (Certificate status export)**, and **FDP_CIMC_OCSP.1 (OCSP basic response validation)** which ensure that certificate revocation lists and certificate status information are valid. In the case that the TOE maintains a copy of the certificate subject's private key**, FDP_ACF_CIMC.2 (User private key confidentiality protection)** ensures that the certificate is not invalidated by the disclosure of the private key by the TOE. In the case that a secret key is used by the certificate subject as an authenticator in requesting a certificate, **FDP_ACF_CIMC.3 (User secret key confidentiality protection)** ensures that an attacker can not obtain a bad certificate by obtaining a user's authenticator from the TOE and then using that authenticator to obtain a bad certificate.

O.Detect modifications of firmware, software, and backup data is provided by **FDP_CIMC_BKP.2 (Extended CIMC backup and recovery)** which covers the requirement that modifications to backup data be detected while **FPT_TST_CIMC.2 (Software/firmware integrity test)** covers the requirement that modifications to software or firmware be detected. Since these **FDP_CIMC_BKP.2** and **FPT_TST_CIMC.2** make use of digital signatures, keyed hashes, or authentication code to detect modifications, **FMT_MTD_CIMC.4 (TSF private key confidentiality protection)** and **FMT_MTD_CIMC.5 (TSF secret key confidentiality protection)** are necessary to ensure that an attacker who has modified firmware, software, or backup data can not prevent detection of the modification by computing a new digital signature, keyed hash, or authentication code.

O.Limitation of administrative access is provided by **FDP_ACC.1 (Subset access control)**, **FDP_ACF.1 (Security attribute based access control)**, **FIA_UAU.1 (Timing of authentication)**, and **FIA_UID.1 (Timing of identification)**. **FIA_UAU.1 (Timing of authentication)** and **FIA_UID.1 (Timing of identification)** ensure that Administrators, Operators, Officers, and Auditors can not perform any security-relevant operations until they have been identified and authenticated and **FDP_ACC.1 (Subset access control)** and **FDP_ACF.1 (Security attribute based access control)** ensure that Administrators, Operators, Officers, and Auditors can only perform those operations necessary to perform their jobs.

O.Maintain user attributes is provided by **FIA_ATD.1 (User attribute definition)** and **FIA_USB.1 (User-subject binding)** which cover the requirement to maintain a set of security attributes associated with individual users and/or subjects acting on users' behalves. **FMT_MSA.1 (Management of security attributes)** ensures that only authorized users can modify security attributes.

O.Respond to possible loss of stored audit records is provided by **FAU_STG.4 (Prevention of audit data loss)** which covers the requirement that no auditable events, except those taken by the Auditor, can be performed when audit trail storage is full.

O.Restrict actions before authentication is provided by **FIA_UAU.1 (Timing of authentication)** which covers the requirement that no security-relevant actions are performed on behalf of a user until that user has been authenticated.

O.Security roles is provided by **FMT_SMR.2 (Restrictions on security roles)** which covers the requirement that security-relevant roles be maintained and that users be associated with those roles.

O.Security-relevant configuration management is provided by **FMT_MSA.2 (Secure security attributes)** and **FMT_MSA.3 (Static attribute initialisation)** which cover the requirement that security attributes have secure values. **FMT_MOF.1 (Management of security functions behavior)** ensures that security-relevant configuration data can only be modified by those who are authorized to do so.

O.User authorization management is provided by **FMT_MSA.1 (Management of security attributes)** which covers the requirement that Administrators manage and update user's security attributes.

System Failures

O.Configuration Management is provided by **FMT_MOF.1 (Management of security functions behavior**) which covers the requirement that only authorized users can change the configuration of the system. **FMT_MOF_CIMC.2 (Certificate profile management)** and **FMT_MOF_CIMC.3 (Extended certificate profile management)** cover the requirement that Administrators be able to control the types of information that are included in generated certificates. **FMT_MOF_CIMC.4 (Certificate revocation list profile management)** and **FMT_MOF_CIMC.5 (Extended certificate revocation list profile management)** cover the requirement that Administrators be able to control to the types of information that are included in generated certificate revocation lists. **FMT_MOF_CIMC.6 (OCSP Profile Management)** covers the requirement that Administrators be able to control to the types of information that are included in generated OCSP responses.

O.Examine source code for developer flaws is provided by **ADV_IMP.1 (Subset of the implementation of the TSF)** which covers the requirement that source code be examined for flaws.

O.Integrity protection of user data and software is provided by **FDP_ITT.1 (Basic internal transfer protection)** and **FDP_SDI_CIMC.3 (Stored public key integrity monitoring and action)** which cover the requirement that user data be protected and **FPT_TST_CIMC.2 (Software/firmware integrity test)** and **FPT_TST_CIMC.3 (Software/firmware load test)** which cover the requirement that software and firmware be protected. Since data and software are protected using cryptography, **FMT_MTD_CIMC.4 (TSF private key confidentiality protection)** and **FMT_MTD_CIMC.5 (TSF secret key confidentiality protection)** are required to protect the confidentiality of the private and secret keys used to protect the data and software.

O.Lifecycle security is provided by **ADV_FSP.1 (Informal functional specification)**, **ADV_FSP.2 (Fully defined external interfaces)**, **ADV_HLD.1 (Descriptive high-level design)**, **ADV_HLD.2 (Security enforcing high-level design)**, **ADV_IMP.1 (Subset of the implementation of the TSF), ADV_INT.1 (Modularity)**, **ADV_LLD.1 (Descriptive low-level design)**, **ADV_RCR.1 (Informal correspondence demonstration)**, and **ADV_SPM.1 (Information TOE security policy model)** which cover the requirement that security is designed into the CIMC. **ALC_FLR.2 (Flaw reporting procedures)** and **ALC_FLR.3 (Systematic flaw remediation)** cover the requirement that flaws are detected and resolved during the operational phase.

O.Manage behavior of security functions is provided by **FMT_MOF.1 (Management of security functions behavior)** which covers the requirement that authorized users be able to configure, operate, and maintain the security mechanisms.

O.Object and data recovery free from malicious code is provided by **FDP_CIMC_BKP.1 (CIMC backup and recovery)**, **FDP_CIMC_BKP.2 (Extended CIMC backup and recovery)**, and **FDP_CIMC_BKP.3 (Advanced CIMC backup and recovery)** which cover the requirement to be able to recover to a viable state and **FPT_TST_CIMC.2 (Software/firmware integrity test)** and **FPT_TST_CIMC.3 (Software/firmware load test)** which cover the requirement that the recovered state is free from malicious code.

O.Periodically check integrity is provided by **FPT_AMT.1 (Abstract machine testing)** which covers the requirement provide periodic integrity checks on the system and **FPT_TST_CIMC.2 (Software/firmware integrity test)** and **FPT_TST_CIMC.3 (Software/firmware load test)** cover the requirement to periodically check the integrity of software.

O.Preservation/trusted recovery of secure state is provided by **FDP_CIMC_BKP.1 (CIMC backup and recovery)** and **FDP_CIMC_BKP.3 (Advanced CIMC backup and recovery)** which cover the requirement that the state of the system be preserved so that it can be recovered in the event of a secure component failure.

O.Procedures for preventing malicious code is provided by **FPT_TST_CIMC.2 (Software/firmware integrity test)** which ensures that only signed code can be executed and **AGD_ADM.1 (Administrator**

Guidance) and **AGD_USR.1 (User Guidance)** which ensure that those who are capable of signing code are trained not to sign malicious code.

O.Protect stored audit records is provided by **FAU_STG.1 (Protected audit trail storage)** which covers the requirement that audit records be protected against modification or unauthorized deletion and **FMT_MTD.1 (Management of TSF data)** which covers the requirement that audit records be protected from unauthorized access. At Security Levels 2-4, where the threat of malicious activity is greater, **FPT_CIMC_TSP.1 (Audit log signing event)** is required so that modifications to the audit logs can be detected.

O.Protect user and TSF data during internal transfer is provided by **FDP_ITT.1 (Basic internal transfer protection)** which covers the requirement that user data be protected during internal transfer and **FPT_ITT.1 (Basic internal TSF data transfer protection)** which covers the requirement that TSF data be protected during internal transfer.

O.Repair identified security flaws is provided by **ALC_FLR.2 (Flaw reporting procedures)** and **ALC_FLR.3 (Systematic Flaw remediation)** which cover the requirement that vendor repair security flaws that have been identified by a user.

O.Require inspection for downloads is provided by **FPT_TST_CIMC.3 (Software/firmware load test)** which covers the requirement that downloaded software can not be loaded until it has been inspected and signed.

O.Sufficient backup storage and effective restoration is provided by **FDP_CIMC_BKP.1 (CIMC backup and recovery)** and **FDP_CIMC_BKP.3 (Advanced CIMC backup and recovery)** which covers the requirement that sufficient backup data is created and stored and that an effective restoration procedure is provided.

O.Time stamps is provided by **FPT_CIMC_TSP.2 (Audit log time stamp event)** which covers the requirement that audit logs are time stamped. **FPT_STM.1 (Reliable time stamps)** covers the requirement that the time stamps be reliable.

O.Validation of security function is provided by **FPT_AMT.1 (Abstract machine testing)** which covers the requirement to ensure that security-relevant hardware and firmware are functioning correctly and **FPT_TST_CIMC.2 (Software/firmware integrity test)** which covers the requirement to ensure that security-relevant software is functioning correctly.

Cryptography

O.Cryptographic functions is provided by **FCS_CKM.1 (Cryptographic key generation)** and **FCS_COP.1 (Cryptographic operation)** which cover the requirement that approved algorithms be used for encryption/decryption, authentication, and signature generation/verification and that approved key generation techniques be used. **AVA_SOF.1 (Strength of TOE security function evaluation)** covers the requirement that FIPS 140 validated cryptographic modules be used.

O.Non-repudiation is provided by **FCO_NRO_CIMC.3 (Enforced proof of origin and verification of origin)** which covers the requirement that messages containing security-relevant data are not accepted by the TOE unless they contain evidence of origin and **FCO_NRO_CIMC.4 (Advanced verification of origin)** which covers the requirement that digital signatures be used so that the evidence of origin for a message may be verified by a third-party.

External Attacks

O.Control unknown source communication traffic is provided by **FCO_NRO_CIMC.3 (Enforced proof of origin and verification of origin)** which covers the requirement that the TOE discard messages from an unknown source that contain security-relevant information.

O.Data import/export is provided by **FDP_ETC_CIMC.4 (User private and secret key export)**, **FDP_ETC_CIMC.5 (Extended user private and secret key export)**, **FMT_MTD_CIMC.6 (TSF private and secret key export)**, and **FMT_MTD_CIMC.7 (Extended TSF private and secret key export)** which cover the requirement that private and secret keys be protected when they are transmitted to and from the TOE. **FDP_UCT.1 (Basic data exchange confidentiality)** and **FPT_ITC.1 (Inter-TSF**

confidentiality during transmission) cover the requirement that data other than private and secret keys be protected when they are transmitted and from the TOE.

O.General user documentation is provided by **AGD_USR.1 (User Guidance)** which covers the requirement that documentation be provided for the general user and for the administrative roles.

O.React to detected attacks is provided by **FIA_AFL.1 (Authentication failure handling)** which covers the requirement that the TSF respond to detected attacks (in the form of repeated authentication attempts) by taking actions to prevent the attacker from successfully authenticating him/herself. In the case that an attack is detected by an Administrator, Auditor, Officer, or Operator, **FCS_CKM.4 (Cryptographic key destruction)** and **FCS_CKM_CIMC.5 (CIMC private and secret key zeroization)** cover the requirement that user who detected the attack be able to destroy and plaintext keys within the TOE in order to prevent the attacker from obtaining copies of these keys.

O.Trusted Path is provided by **FTP_TRP.1 (Trusted path)** which covers the requirement that a trusted path between the user and the system be provided.

8.4 Internal Consistency and Mutual Support

This section demonstrates that the stated security requirements together form a mutually supportive and internally consistent whole. Internal consistency is demonstrated in an analysis of dependencies. Mutual support is shown through consideration of the interactions between and among the SFRs.

8.4.1 Rationale that Dependencies are Satisfied

The selected security requirements include related dependencies, both direct and indirect. The indirect dependencies are those required by the direct dependencies. All of these dependencies must be met or their exclusion justified.

8.4.1.1 Security Functional Requirements Dependencies

The following tables provide a summary of the security functional requirements dependency analysis for each security level.

8.4.1.1.1 Security Level 1

Table 17. Summary of Security Functional Requirements Dependencies for Security Level 1

Component	Dependencies	Which is:
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation	Included
	FIA_UID.1 Timing of identification	Included
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	Included
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	Included
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation	Included
	FMT_MTD.1 Management of TSF data	Included
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	Included
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	Included
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	FIA_UID.1 Timing of identification	Included
FCS_CKM.1 Cryptographic key generation	FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation	FCS_COP.1 Included
	FCS_CKM.4 Cryptographic key destruction	Included
	FMT_MSA.2 Secure security attributes	NOT Included

Table 17. Summary of Security Functional Requirements Dependencies for Security Level 1

Component	Dependencies	Which is:
FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	NOT Included
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	None	
FCS_COP.1 Cryptographic operation	FCS_CKM.4 Cryptographic key destruction	Included
	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	NOT Included
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	Included
	FMT_MSA.3 Static attribute initialization	Included
FDP_ACF_CIMC.2 User private key confidentiality protection	None	
FDP_ACF_CIMC.3 User secret key confidentiality protection	None	
FDP_CIMC_BKP.1 CIMC backup and recovery	None	
FDP_CIMC_CER.1 Certificate Generation	None	
FDP_CIMC_CRL.1 Certificate revocation list validation	None	
FDP_CIMC_CSE.1 Certificate status export	None	
FDP_CIMC_OCSP.1 OCSP basic response validation	None	
FDP_ETC_CIMC.4 User private and secret key export	None	
FDP_ITT.1 Basic internal transfer protection	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	None	
FDP_UCT.1 Basic data exchange confidentiality	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	Included
	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path	NOT Included
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	Included
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)

Table 17. Summary of Security Functional Requirements Dependencies for Security Level 1

Component	Dependencies	Which is:
FMT_MOF_CIMC.2 Certificate profile management	None	
FMT_MOF_CIMC.4 Certificate revocation list profile management	None	
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	FMT_MOF_CIMC.4	Included
FMT_MOF_CIMC.6 OCSP profile management	None	
FMT_MSA.1 Management of security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD_CIMC.4 TSF private key confidentiality protection	None	
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	None	
FMT_MTD_CIMC.6 TSF private and secret key export	None	
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification	Included
FPT_AMT.1 Abstract machine testing	None	
FPT_ITC.1 Inter-TSF confidentiality during transmission	None	
FPT_ITT.1 Basic internal TSF data transfer protection	None	
FPT_STM.1 Reliable time stamps	None	
FPT_TST_CIMC.2 Software/firmware integrity test	FPT_AMT.1 Abstract machine testing	Included
FPT_TST_CIMC.3 Software/firmware load test	FPT_AMT.1 Abstract Machine Testing	Included

8.4.1.1.1.1 Justification of Unsupported Dependencies Regarding FMT_MSA.2

Components FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction, and FCS_COP.1 Cryptographic operation have direct dependencies on FMT_MSA.2 that are unmet. This security level requires use of a FIPS 140 validated cryptographic module. All of the dependencies listed are part of the cryptographic module. Therefore, the dependency on FMT_MSA.2 is not applicable.

8.4.1.1.1.2 Justification of Unsupported Dependencies Regarding FTP_ITC.1 or FTP_TRP.1

Component FDP_UCT.1 Basic data exchange confidentiality has a direct dependency on FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path that is unmet. This product uses basic encryption to

ensure basic data exchange confidentiality. It is unnecessary for this product to require Inter-TSF trusted channel or trusted path at this security level.

8.4.1.1.2 Security Level 2

Table 18. Summary of Security Functional Requirements Dependencies for Security Level 2

Component	Dependencies	Which is:
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation	Included
	FIA_UID.1 Timing of identification	Included
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	Included
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	Included
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation	Included
	FMT_MTD.1 Management of TSF data	Included
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	Included
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	Included
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	FIA_UID.1 Timing of identification	Included
FCS_CKM.1 Cryptographic key generation	FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation	FCS_COP.1 Included
	FCS_CKM.4 Cryptographic key destruction	Included
	FMT_MSA.2 Secure security attributes	Included
FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	Included
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	None	
FCS_COP.1 Cryptographic operation	FCS_CKM.4 Cryptographic key destruction	Included
	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	Included
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	Included
	FMT_MSA.3 Static attribute initialization	Included
FDP_ACF_CIMC.2 User private key confidentiality protection	None	
FDP_ACF_CIMC.3 User secret key confidentiality protection	None	
FDP_CIMC_BKP.1 CIMC backup and recovery	None	
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	FDP_CIMC_BKP.1 CIMC backup and recovery	Included
FDP_CIMC_CER.1 Certificate Generation	None	

Table 18. Summary of Security Functional Requirements Dependencies for Security Level 2

Component	Dependencies	Which is:
FDP_CIMC_CRL.1 Certificate revocation list validation	None	
FDP_CIMC_CSE.1 Certificate status export	None	
FDP_CIMC_OCSP.1 OCSP basic response validation	None	
FDP_ETC_CIMC.4 User private and secret key export	None	
FDP_ITT.1 Basic internal transfer protection	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	None	
FDP_UCT.1 Basic data exchange confidentiality	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	Included
	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path	NOT Included
FIA_AFL.1 Authentication failure handling	FIA_UAU.1 Timing of authentication	Included
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	Included
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MOF_CIMC.2 Certificate profile management	None	
FMT_MOF_CIMC.3 Extended certificate profile management	FMT_MOF_CIMC.2	Included
FMT_MOF_CIMC.4 Certificate revocation list profile management	None	
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	FMT_MOF_CIMC.4	Included
FMT_MOF_CIMC.6 OCSP profile management	None	
FMT_MSA.1 Management of security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.2 Secure security attributes	ADV_SPM.1 Informal TOE security policy model	Included
	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security Roles	Included (hierarchical to FMT_SMR.2)

Table 18. Summary of Security Functional Requirements Dependencies for Security Level 2

Component	Dependencies	Which is:
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD_CIMC.4 TSF private key confidentiality protection	None	
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	None	
FMT_MTD_CIMC.6 TSF private and secret key export	None	
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification	Included
FPT_AMT.1 Abstract machine testing	None	
FPT_CIMC_TSP.1 Audit log signing event	FAU_GEN.1	Included
FPT_ITC.1 Inter-TSF confidentiality during transmission	None	
FPT_ITT.1 Basic internal TSF data transfer protection	None	
FPT_STM.1 Reliable time stamps	None	
FPT_TST_CIMC.2 Software/firmware integrity test	FPT_AMT.1 Abstract machine testing	Included
FPT_TST_CIMC.3 Software/firmware load test	FPT_AMT.1 Abstract Machine Testing	Included

8.4.1.1.2.1 Justification of Unsupported Dependencies Regarding FTP_ITC.1 or FTP_TRP.1

Component FDP_UCT.1 Basic data exchange confidentiality has a direct dependency on FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path that is unmet. This product uses basic encryption to ensure basic data exchange confidentiality. It is unnecessary for this product to require Inter-TSF trusted channel or trusted path at this security level.

8.4.1.1.3 Security Level 3

Table 19. Summary of Security Functional Requirements Dependencies for Security Level 3

Component	Dependencies	Which is:
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation	Included
	FIA_UID.1 Timing of identification	Included
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	Included
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	Included
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation	Included
	FMT_MTD.1 Management of TSF data	Included
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	Included
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	Included

Table 19. Summary of Security Functional Requirements Dependencies for Security Level 3

Component	Dependencies	Which is:
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	FIA_UID.1 Timing of identification	Included
FCO_NRO_CIMC.4 Advanced verification of origin	FCO_NRO_CIMC.3	Included
FCS_CKM.1 Cryptographic key generation	FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation	FCS_COP.1 Included
	FCS_CKM.4 Cryptographic key destruction	Included
	FMT_MSA.2 Secure security attributes	Included
FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	Included
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	None	
FCS_COP.1 Cryptographic operation	FCS_CKM.4 Cryptographic key destruction	Included
	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	Included
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	Included
	FMT_MSA.3 Static attribute initialization	Included
FDP_ACF_CIMC.2 User private key confidentiality protection	None	
FDP_ACF_CIMC.3 User secret key confidentiality protection	None	
FDP_CIMC_BKP.1 CIMC backup and recovery	None	
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	FDP_CIMC_BKP.1 CIMC backup and recovery	Included
FDP_CIMC_CER.1 Certificate Generation	None	
	None	
FDP_CIMC_CSE.1 Certificate status export	None	
FDP_CIMC_OCSP.1 OCSP basic response validation	None	
FDP_CIMC_POP.1 Proof of possession for key management keys	None	
FDP_ETC_CIMC.4 User private and secret key export	None	
FDP_ETC_CIMC.5 Extended user private and secret key export	FDP_ETC_CIMC.4	Included
FDP_ITT.1 Basic internal transfer protection	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included

Table 19. Summary of Security Functional Requirements Dependencies for Security Level 3

Component	Dependencies	Which is:
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	None	
FDP_UCT.1 Basic data exchange confidentiality	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	Included
	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path	NOT Included
FIA_AFL.1 Authentication failure handling	FIA_UAU.1 Timing of authentication	Included
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	Included
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MOF_CIMC.2 Certificate profile management	None	
FMT_MOF_CIMC.3 Extended certificate profile management	FMT_MOF_CIMC.2	Included
FMT_MOF_CIMC.4 Certificate revocation list profile management	None	
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	FMT_MOF_CIMC.4	Included
FMT_MOF_CIMC.6 OCSP profile management	None	
FMT_MSA.1 Management of security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.2 Secure security attributes	ADV_SPM.1 Informal TOE security policy model	Included
	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security Roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD_CIMC.4 TSF private key confidentiality protection	None	
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	None	
FMT_MTD_CIMC.6 TSF private and secret key export	None	

Table 19. Summary of Security Functional Requirements Dependencies for Security Level 3

Component	Dependencies	Which is:
FMT_MTD_CIMC.7 Extended TSF private and secret key export	FMT_MTD_CIMC.6	Included
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification	Included
FPT_AMT.1 Abstract machine testing	None	
FPT_CIMC_TSP.1 Audit log signing event	FAU_GEN.1	Included
FPT_ITC.1 Inter-TSF confidentiality during transmission	None	
FPT_ITT.1 Basic internal TSF data transfer protection	None	
FPT_STM.1 Reliable time stamps	None	
FPT_TST_CIMC.2 Software/firmware integrity test	FPT_AMT.1 Abstract machine testing	Included
FPT_TST_CIMC.3 Software/firmware load test	FPT_AMT.1 Abstract Machine Testing	Included
FTP_TRP.1 Trusted path	None	

8.4.1.1.3.1 Justification of Unsupported Dependencies Regarding FTP_ITC.1 or FTP_TRP.1

Component FDP_UCT.1 Basic data exchange confidentiality has a direct dependency on FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path that is unmet. This product uses basic encryption to ensure basic data exchange confidentiality. It is unnecessary for this product to require Inter-TSF trusted channel or trusted path at this security level.

8.4.1.1.4 Security Level 4

Table 20. Summary of Security Functional Requirements Dependencies for Security Level 4

Component	Dependencies	Which is:
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation	Included
	FIA_UID.1 Timing of identification	Included
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	Included
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	Included
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation	Included
	FMT_MTD.1 Management of TSF data	Included
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	Included
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	Included
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	FIA_UID.1 Timing of identification	Included
FCO_NRO_CIMC.4 Advanced verification of origin	FCO_NRO_CIMC.3	Included

Table 20. Summary of Security Functional Requirements Dependencies for Security Level 4

Component	Dependencies	Which is:
FCS_CKM.1 Cryptographic key generation	FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation	FCS_COP.1 Included
	FCS_CKM.4 Cryptographic key destruction	Included
	FMT_MSA.2 Secure security attributes	Included
FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	Included
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	None	
FCS_COP.1 Cryptographic operation	FCS_CKM.4 Cryptographic key destruction	Included
	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	Included
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	Included
	FMT_MSA.3 Static attribute initialization	Included
FDP_ACF_CIMC.2 User private key confidentiality protection	None	
FDP_ACF_CIMC.3 User secret key confidentiality protection	None	
FDP_CIMC_BKP.1 CIMC backup and recovery	None	
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	FDP_CIMC_BKP.1 CIMC backup and recovery	Included
FDP_CIMC_BKP.3 Advanced CIMC backup and recovery	FDP_CIMC_BKP.1 CIMC backup and recovery	Included
	FDP_CIMC_BKP.2 Extended CIMC backup and recovery	Included
FDP_CIMC_CER.1 Certificate Generation	None	
FDP_CIMC_CRL.1 Certificate revocation list validation	None	
FDP_CIMC_CSE.1 Certificate status export	None	
FDP_CIMC_OCSP.1 OCSP basic response validation	None	
FDP_CIMC_POP.1 Proof of possession for key management keys	None	
FDP_ETC_CIMC.4 User private and secret key export	None	
FDP_ETC_CIMC.5 Extended user private and secret key export	FDP_ETC_CIMC.4	Included

Table 20. Summary of Security Functional Requirements Dependencies for Security Level 4

Component	Dependencies	Which is:
FDP_ITT.1 Basic internal transfer protection	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	None	
FDP_UCT.1 Basic data exchange confidentiality	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	Included
	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path	FTP_TRP.1 Included
FIA_AFL.1 Authentication failure handling	FIA_UAU.1 Timing of authentication	Included
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	Included
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MOF_CIMC.2 Certificate profile management	None	
FMT_MOF_CIMC.3 Extended certificate profile management	FMT_MOF_CIMC.2	Included
FMT_MOF_CIMC.4 Certificate revocation list profile management	None	
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	FMT_MOF_CIMC.4	
FMT_MOF_CIMC.6 OCSP profile management	None	
FMT_MSA.1 Management of security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.2 Secure security attributes	ADV_SPM.1 Informal TOE security policy model	Included (hierarchical to FMT_SMR.2)
	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security Roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD_CIMC.4 TSF private key confidentiality protection	None	

Table 20. Summary of Security Functional Requirements Dependencies for Security Level 4

Component	Dependencies	Which is:
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	None	
FMT_MTD_CIMC.6 TSF private and secret key export	None	
FMT_MTD_CIMC.7 Extended TSF private and secret key export	FMT_MTD_CIMC.6	Included
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification	Included
FPT_AMT.1 Abstract machine testing	None	
FPT_CIMC_TSP.1 Audit log signing event	FAU_GEN.1	Included
FPT_CIMC_TSP.2 Audit log time stamp event	FAU_GEN.1	Included
FPT_ITC.1 Inter-TSF confidentiality during transmission	None	
FPT_ITT.1 Basic internal TSF data transfer protection	None	
FPT_STM.1 Reliable time stamps	None	
FPT_TST_CIMC.2 Software/firmware integrity test	FPT_AMT.1 Abstract machine testing	Included
FPT_TST_CIMC.3 Software/firmware load test	FPT_AMT.1 Abstract Machine Testing	Included
FTP_TRP.1 Trusted path	None	

8.4.1.2 Security Assurance Requirements Dependencies

The following tables provide a summary of the security assurance requirements dependency analysis for each security level.

Table 21. Summary of Security Assurance Requirements Dependencies for Security Level 1

Component	Depends On:	Which is:
ACM_CAP.1	no dependencies	Not applicable
ADO_IGS.1	AGD_ADM.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
ADV_FSP.1	ADV_RCR.1	included
ADV_RCR.1	no dependencies	not applicable
AGD_ADM.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
AGD_USR.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)

Table 21. Summary of Security Assurance Requirements Dependencies for Security Level 1

Component	Depends On:	Which is:
	(indirect) ADV_RCR.1	included
ATE_FUN.1	no dependencies	not applicable
ATE_IND.1	ADV_FSP.1	Included
	AGD_ADM.1	Included
	AGD_USR.1	included
AVA_SOF.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_HLD.1	included (hierarchical to ADV_HLD.2)
	(indirect) ADV_RCR.1	included

Table 22. Summary of Security Assurance Requirements Dependencies for Security Level 2

Component	Depends On:	Which is:
ACM_CAP.3	ACM_SCP.1	Included (hierarchical to ACM_SCP.2)
	ALC_DVS.1	included
ACM_SCP.2	ACM_CAP.3	included (hierarchical to ACM_CAP.4)
	(indirect) ALC_DVS.1	included
ADO_DEL.1	no dependencies	
ADO_IGS.1	AGD_ADM.1	included
	(indirect) ADV_FSP.1	included
	(indirect) ADV_RCR.1	included
ADV_FSP.1	ADV_RCR.1	included
ADV_HLD.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_RCR.1	included
ADV_RCR.1	no dependencies	not applicable
ADV_SPM.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
AGD_ADM.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included

Table 22. Summary of Security Assurance Requirements Dependencies for Security Level 2

Component	Depends On:	Which is:
AGD_USR.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
ALC_DVS.1	no dependencies	not applicable
ALC_FLR.2	no dependencies	not applicable
ATE_COV.2	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ATE_FUN.1	included
	(indirect) ADV_RCR.1	included
ATE_DPT.1	ADV_HLD.1	included (hierarchical to ADV_HLD.2)
	ATE_FUN.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
ATE_FUN.1	no dependencies	not applicable
ATE_IND.2	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	AGD_ADM.1	included
	AGD_USR.1	included
	ATE_FUN.1	included
	(indirect) ADV_RCR.1	included
AVA_MSU.2	ADO_IGS.1	included
	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	AGD_ADM.1	included
	AGD_USR.1	included
	(indirect) ADV_RCR.1	included
AVA_SOF.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_HLD.1	included (hierarchical to ADV_HLD.2)
	(indirect) ADV_RCR.1	included
AVA_VLA.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_HLD.1	included

Table 22. Summary of Security Assurance Requirements Dependencies for Security Level 2

Component	Depends On:	Which is:
	AGD_ADM.1	included
	AGD_USR.1	included

Table 23. Summary of Security Assurance Requirements Dependencies for Security Level 3

Component	Depends On:	Which is:
ACM_CAP.3	ACM_SCP.1	Included (hierarchical to ACM_SCP.2)
	ALC_DVS.1	included
ACM_SCP.2	ACM_CAP.3	included (hierarchical to ACM_CAP.4)
	(indirect) ALC_DVS.1	included
ADO_DEL.2	ACM_CAP.3	included (hierarchical to ACM_CAP.4)
	(indirect) ACM_SCP.1	included (hierarchical to ACM_SCP.2)
	(indirect) ALC_DVS.1	included
ADO_IGS.1	AGD_ADM.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
ADV_HLD.2	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_RCR.1	included
ADV_IMP.1	ADV_LLD.1	included
	ADV_RCR.1	included
	ALC_TAT.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_HLD.2	included
ADV_LLD.1	ADV_HLD.2	included
	ADV_RCR.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
ADV_RCR.1	no dependencies	not applicable

Table 23. Summary of Security Assurance Requirements Dependencies for Security Level 3

Component	Depends On:	Which is:
ADV_SPM.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
AGD_ADM.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
AGD_USR.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
ALC_DVS.1	no dependencies	not applicable
ALC_FLR.2	no dependencies	not applicable
ALC_TAT.1	ADV_IMP.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_HLD.2	included
	(indirect) ADV_LLD.1	included
	(indirect) ADV_RCR.1	included
ATE_COV.2	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ATE_FUN.1	included
	(indirect) ADV_RCR.1	included
ATE_DPT.1	ADV_HLD.1	included (hierarchical to ADV_HLD.2)
	ATE_FUN.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
ATE_FUN.1	no dependencies	not applicable
ATE_IND.2	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	AGD_ADM.1	included
	AGD_USR.1	included
	ATE_FUN.1	included
	(indirect) ADV_RCR.1	included
AVA_MSU.2	ADO_IGS.1	included

Table 23. Summary of Security Assurance Requirements Dependencies for Security Level 3

Component	Depends On:	Which is:
	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	AGD_ADM.1	included
	AGD_USR.1	included
	(indirect) ADV_RCR.1	included
AVA_SOF.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_HLD.1	included (hierarchical to ADV_HLD.2)
	(indirect) ADV_RCR.1	included
AVA_VLA.2	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_HLD.2	included
	ADV_IMP.1	included
	ADV_LLD.1	included
	AGD_ADM.1	included
	AGD_USR.1	included
	(indirect) ADV_RCR.1	included
	(indirect) ALC_TAT.1	included

Table 24. Summary of Security Assurance Requirements Dependencies for Security Level 4

Component	Depends On:	Which is:
ACM_AUT.1	ACM_CAP.3	included (hierarchical to ACM_CAP.4)
	(indirect) ACM_SCP.1	included (hierarchical to ACM_SCP.2)
	(indirect) ALC_DVS.1	included
ACM_CAP.4	ACM_SCP.1	included (hierarchical to ACM_SCP.2)
	ALC_DVS.1	included
ACM_SCP.2	ACM_CAP.3	included (hierarchical to ACM_CAP.4)
	(indirect) ALC_DVS.1	included
ADO_DEL.2	ACM_CAP.3	included (hierarchical to ACM_CAP.4)

Table 24. Summary of Security Assurance Requirements Dependencies for Security Level 4

Component	Depends On:	Which is:
	(indirect) ACM_SCP.1	included (hierarchical to ACM_SCP.2)
	(indirect) ALC_DVS.1	included
ADO_IGS.1	AGD_ADM.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
ADV_FSP.2	ADV_RCR.1	included
ADV_HLD.2	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_RCR.1	included
ADV_IMP.1	ADV_LLD.1	included
	ADV_RCR.1	included
	ALC_TAT.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_HLD.2	included
ADV_INT.1	ADV_IMP.1	included
	ADV_LLD.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_HLD.2	included
	(indirect) ADV_RCR.1	included
	(indirect) ALC_TAT.1	included
ADV_LLD.1	ADV_HLD.2	included
	ADV_RCR.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
ADV_RCR.1	no dependencies	not applicable
ADV_SPM.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
AGD_ADM.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included

Table 24. Summary of Security Assurance Requirements Dependencies for Security Level 4

Component	Depends On:	Which is:
AGD_USR.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
ALC_DVS.1	no dependencies	not applicable
ALC_FLR.3	no dependencies	not applicable
ALC_LCD.1	no dependencies	not applicable
ALC_TAT.1	ADV_IMP.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_HLD.2	included
	(indirect) ADV_LLD.1	included
	(indirect) ADV_RCR.1	included
ATE_COV.2	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ATE_FUN.1	included
	(indirect) ADV_RCR.1	included
ATE_DPT.2	ADV_HLD.2	included (hierarchical to ADV_HLD.2)
	ADV_LLD.1	included
	ATE_FUN.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
ATE_FUN.1	no dependencies	not applicable
ATE_IND.2	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	AGD_ADM.1	included
	AGD_USR.1	included
	ATE_FUN.1	included
	(indirect) ADV_RCR.1	included
AVA_MSU.2	ADO_IGS.1	included
	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	AGD_ADM.1	included

Table 24. Summary of Security Assurance Requirements Dependencies for Security Level 4

Component	Depends On:	Which is:
	AGD_USR.1	included
	(indirect) ADV_RCR.1	included
AVA_SOF.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_HLD.1	included (hierarchical to ADV_HLD.2)
	(indirect) ADV_RCR.1	included
AVA_VLA.3	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_HLD.2	included
	ADV_IMP.1	included
	ADV_LLD.1	included
	AGD_ADM.1	included
	AGD_USR.1	included
	(indirect) ADV_RCR.1	included
	(indirect) ALC_TAT.1	included

8.4.2 Rationale that Requirements are Mutually Supportive

The requirements represented in this PP were developed from a variety of sources. The security requirements work mutually so that each SFR is protected against bypassing, tampering, deactivation, and detection attacks by other SFRs.

8.4.2.1 Bypass

Prevention of bypass is derived as described below:

FIA_UID.1 and FIA_UAU.1 support other functions' allowing user access to data by limiting the actions the user can take prior to identification and authentication.

The management functions, including FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1 support all other SFRs by restricting the ability to change certain management functions to certain specified roles, thus ensuring that other users cannot circumvent these SFRs.

FMT_MSA.2 and FMT_MSA.3 limit the acceptable values for secure data, thus providing protection from bypass to those SFRs dependent on that data.

FPT_FLS.1, FPT_RCV.3 and FPT_RCV.4 provide for maintenance and recovery of a secure state after failure or service discontinuity, thus preventing bypass of other SFRs.

FPT_TST_CIMC.2 provides for integrity testing to ensure that selected security functions are operational, thus checking for bypass.

8.4.2.2 Tamper

Prevention of tamper is derived as described below:

FAU_STG.1 protects the integrity of the audit trail.

FCS_CKM.1 and FCS_COP.1 provide for the secure generation and handling of keys, and therefore support those SFRs that may rely on the use of those keys.

FDP_ETC_CIMC.4 and FDP_ETC_CIMC.5 prevent modification errors during export of secret and/or private keys.

FIA_AFL.1 supports all SFRs dealing with authentication by limiting the number of entry attempts, and then mandating an appropriate action to protect the TOE if too many attempts have been made.

FIA_UID.1 and FIA_UAU.1 support other functions allowing user access to data by limiting the actions the user can take prior to identification and authentication.

The management functions, including FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1 support all other SFRs by restricting the ability to change certain management functions to certain specified roles, thus ensuring that other users cannot circumvent these SFRs.

FMT_MSA.2 and FMT_MSA.3 limit the acceptable values for secure data, thus providing protection from tampering to those SFRs dependent on that data.

FPT_TST_CIMC.2 provides for integrity testing to ensure that selected security functions are operational, thus checking for tampering.

8.4.2.3 Deactivation

Prevention of deactivation is derived as described below:

The access control SFP detailed in FDP_ACF.1 along with the other SFRs dealing with access control, provide for rigorous control of allowed data manipulations and thus prevent unauthorized deactivation.

The management functions, including FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1, support all other SFRs by restricting the ability to change certain management functions to certain specified roles, thus ensuring that other users cannot circumvent these SFRs.

FMT_MSA.2 and FMT_MSA.3 limit the acceptable values for secure data, thus providing protection from deactivation to those SFRs dependent on that data.

FPT_TST_CIMC.2 provides for integrity testing to ensure that selected security functions are operational, thus checking for tampering.

8.4.2.4 Detection

Detection is derived as described below:

The security audit functions, including FAU_GEN.1, FAU_GEN.2, and FAU_SEL.1 provide for the generation of audit data that may be used to detect attempts to defeat specific SFRs or potential misconfiguration that could leave the TOE prone to attack.

FAU_SAR.1 and FAU_SAR.3, support the audit generation SFRs by providing the capability to selectively search the audit records.

FAU_STG.1, and FAU_STG.4 provide for the protection of the audit records.

The management functions, including FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1, support all other SFRs by restricting the ability to change certain management functions to certain specified roles, thus ensuring that other users cannot circumvent these SFRs.

FMT_MSA.2 and FMT_MSA.3 limit the acceptable values for secure data, thus providing detection protection to those SFRs dependent on that data.

FMT_SMR.2 provides for the specification of multiple roles, thus supporting the other detection SFRs.

8.5 *Rationale for Strength of Function*

The TOE described in this protection profile is intended to operate in a range of environments, from benign to hostile. Also, the users may be hostile. Therefore, the TOE requires cryptographic functions to provide for integrity, confidentiality, nondisclosure, and authentication. The authentication strength of function metrics provide for a basic level, and are currently within commercially available products. The cryptographic functions must be included in a cryptographic module that has been validated against FIPS 140, *Security Requirements for Cryptographic Modules*. The specific level required for the cryptographic module depends on the type and use of the key and the CIMC security level. The cryptographic module levels are specified in Table 6. The increasing FIPS 140 level corresponding to the increased CIMC security level, addresses the increased threats and potential for loss at the higher levels.

8.6 Assurance Requirements Rationale

8.6.1 Rationale for Security Level 1

Security Level 1 provides the lowest level of security. CIMCs designed to meet the security requirements at Security Level 1 may be appropriate for use in environments in which the threat of malicious activity is considered to be low. The objective of this assurance level is to provide evidence that the CIMC functions as specified in the associated documentation. The assurance level for this security level is EAL1 augmented. Augmentation results from the selection of:

ATE_FUN.1 Functional testing

EAL1 does not have the ATE_FUN component. This family contributes to providing assurance that the likelihood of undiscovered flaws is relatively small. The rationale for this augmentation is that the developer should perform functional testing and provide test documentation. The testing will provide assurance that the TSF satisfies the functional security requirements. Developer functional testing is supplemented by independent testing performed by the testing laboratory.

AVA_SOF.1 Strength of TOE Security Function Evaluation

EAL1 does not have the AVA_SOF component. This family contributes to the security of probabilistic or permutational mechanisms (e.g. a password or hash function). The rationale for this augmentation is that the developer should provide knowledge about the ability of the related security function to counter the identified threats. This knowledge will provide assurance that the functions meet or exceed the claim. Developer functional testing is supplemented by independent testing performed by the testing laboratory.

8.6.2 Rationale for Security Level 2

CIMCs designed to meet Security Level 2 may be appropriate where the risks and consequences of data disclosure are not significant. CIMCs at Security Level 2 should defend against most attacks initiated through a network. It is assumed at this security level that the users of the PKI are not malicious. The second assurance level for this security level is EAL2 augmented. This assurance level would be EAL3 except for descriptive high-level design.

This assurance level matches the assurance requirements of Guidance for COTS Security Protection Profiles (CSPP). These requirements stress assurance through vendor actions that are currently within best commercial practices. The assurance requirements of CSPP, which shall be referred to as EAL-CSPP, stress assurance through vendor actions that are within the bounds of current best commercial practice. EAL-CSPP provides, primarily via review of vendor supplied evidence, independent confirmation that these actions have been competently performed. EAL-CSPP also includes the following independent, third-party analysis: (1) confirmation of system generation and installation procedures, (2) verification that the system security state is not misrepresented, (3) verification of a sample of the vendor functional testing, (4) searching for obvious vulnerabilities, and (5) independent functional testing.

Augmentation above EAL3 results from the selection of:

ACM_SCP.2 Problem tracking configuration management coverage

A CS2 vendor can be expected to apply configuration management to the items called out in ACM_SCP.2. Specifically, since the product is security related, the tracking of security flaws is a very reasonable expectation and within the bounds of standard, best commercial practice.

ADV_SPM.1 Informal TOE security policy model

While the generation of a security policy does require security expertise, this can be performed by a consultant (if necessary) and does not otherwise impact the vendor's existing development process at this security level.

ALC_FLR.2 Flaw Report Procedures

None of the EAL levels have the ALC_FLR component. It is within best commercial practices for a vendor of security products to have flaw reporting procedures covering:

- Addressing user reported problems
- Correcting flaws
- Notifying users and
- Revising procedures to reduce the potential for introducing new and/or additional flaws.

Specific procedures are not defined in the assurance requirement, therefore this should have minimal impact on vendors who have already implemented a flaw reporting program.

ALC_TAT.1

AVA_MSU.2 Validation of analysis components

A security vendor implementing standard, best commercial practices will not be impacted by this component. AVA_MSU.2 requires that the vendor produce user and administrator documentation that is adequate for understanding the operating modes of the TOE and the required external security controls necessary for secure operation. The vendor is required to analyze this documentation for conformance to the requirements.

8.6.3 Rationale for Security Level 3

CIMCs designed to meet Security Level 3 may be appropriate for environments where risks and consequences of data disclosure and loss of data integrity are moderate. Level 3 requires additional integrity controls to ensure data is not modified. A CIMC at Security Level 3 includes protections to protect against someone with physical access to the components and includes additional assurance requirements to ensure the CIMC is functioning securely.

The assurance level for this security level is EAL3/EAL4 augmented. Augmentation results from the selection of:

ACM_SCP.2 Problem tracking configuration management coverage

A vendor can be expected to apply configuration management to the items called out in ACM_SCP.2. Specifically, since the product is security related, the tracking of security flaws is a very reasonable expectation and within the bounds of standard, best commercial practice.

ADO_DEL.2 Detection of modification

A vendor can be expected to use a signature or other method to ensure that the code has not been tampered with prior to installation. Since the product is security related, this type of precaution should be expected.

ADV_FSP.2 Fully defined external interfaces
It is not a difficult task to fully define all external interfaces to the product. Indeed, this is necessary to correctly develop the product for interaction with other products. This will provide the necessary detail for supporting both thorough testing of the TOE and the assessment of vulnerabilities.

ADV_IMP.1 Subset of the implementation of the TSF

This high a level of assurance requires that additional documentation regarding the implementation of the product be provided. It is through examination of this portion of the implementation that the product can be adequately evaluated with regard to the requirements.

ADV_LLD.1 Descriptive low-level design

This high a level of assurance requires that additional documentation regarding the design of the product be provided. It is through examination of this design that the product can be adequately evaluated with regard to the requirements.

ADV_SPM.1 Informal TOE security policy model

While the generation of a security policy does require security expertise, this can be performed by a consultant (if necessary) and does not otherwise impact the vendor's existing development process at this security level.

ALC_FLR.2 Flaw Report Procedures

EAL3 and EAL4 do not have the ALC_FLR component. It is within best commercial practices for a vendor of security products to have flaw reporting procedures covering:

- Addressing user reported problems
- Correcting flaws
- Notifying users and
- Revising procedures to reduce the potential for introducing new and/or additional flaws.

Specific procedures are not defined in the assurance requirement, therefore this should have minimal impact on vendors who have already implemented a flaw reporting program.

ALC_TAT.1 Well-defined development tools

It is important that very secure products be unambiguous.

AVA_MSU.2 Validation of analysis components

A security vendor implementing standard, best commercial practices will not be impacted by this component. AVA_MSU.2 requires that the vendor produce user and administrator documentation that is adequate for understanding the operating modes of the TOE and the required external security controls necessary for secure operation. The vendor is required to analyze this documentation for conformance to the requirements.

AVA_VLA.2 Independent vulnerability analysis

Penetration attacks are very likely given the threat model for this security level. As a result, it is important that some penetration analysis and testing be performed.

8.6.4 Rationale for Security Level 4

CIMCs designed to meet Security Level 4 may be appropriate where the threats to and consequences of data disclosure and loss of data integrity are significant. The environment and the users may be hostile. Security Level 4 is intended to protect against malicious authorized and unauthorized users.

The assurance level for this security level is EAL4 augmented. Augmentation results from the selection of:

ADV_INT.1 Modularity

The rationale for this augmentation is based on the fact that the TOE is composed of a collection of functions ranging from basic operating functions to advanced applications. These may be developed by different organizations within a company (or by different companies). Consequently, the functions contained in the final product must have the minimum possibility of destructive interactive.

ALC_FLR.3 Systematic Flaw Remediation

EAL4 does not have the ALC_FLR component. Flaw remediation procedures cover:

- Addressing user reported problems
- Identifying and correcting flaws
- Automatic distribution of security flaw reports and the associated corrections and
- Revising procedures to reduce the potential for introducing new and/or additional flaws.

ATE_DPT.2 Testing: low-level design

At Security Level 4, the threats to and consequences of data disclosure and loss of data integrity are significant. In addition, the environment and the users may be hostile. Therefore, the TSF must be tested at a low level. The components in this family address the level of detail to which the TSF is tested. The objective is to counter the risk of missing an error in the development of the TOE. Additionally, the components of this family are more likely to discover any malicious code that has been inserted. Testing at the level of the subsystems and modules provides assurance that the TSF subsystems and modules have been correctly implemented.

AVA_VLA.3 Moderately resistant

At Security Level 4, the threats to and consequences of data disclosure and loss of data integrity are significant. In addition, the environment and the users may be hostile. As a result, the TOE must be shown to be resistant to penetration attacks. EAL4 requires vulnerability assessment through imposition of AVA_VLA.2. This requires a review of only the identified vulnerabilities. Component AVA_VLA.3 requires, in addition, that a systematic search for vulnerabilities be documented and presented. This provides a significant increase in the consideration of vulnerabilities over that provided by AVA_VLA.2.

9 CIMC ACCESS CONTROL POLICY

The TOE shall support the administration and enforcement of a CIMC access control policy that provides the capabilities described below.

Subjects (human users) will be granted access to objects (data/files) based upon the:

1. Identity of the subject requesting access,
2. Role (or roles) the subject is authorized to assume,
3. Type of access requested,
4. Content of the access request, and,
5. Possession of a secret or private key, if required.

Subject identification includes:

- Individuals with different access authorizations
- Roles with different access authorizations
- Individuals assigned to one or more roles with different access authorizations

Access type, with explicit allow or deny:

- Read
- Write
- Execute

For each object, an explicit owning subject and role will be identified. Also, the assignment and management of authorizations will be the responsibility of the owner of an object or a role(s), as specified in this PP.

10 GLOSSARY OF TERMS[4]

The following definitions are used throughout this standard:

Authentication code: a cryptographic checksum, based on a FIPS-approved or recommended security method; also known as a Message Authentication Code (MAC) in ANSI standards.

CIMC: the set of hardware, software, firmware, or some combination thereof, that issues, revokes, and manages public key certificates and certificate status information, and is contained within the CIMC boundary.

CIMC boundary: an explicitly defined contiguous perimeter that establishes the physical bounds of a CIMC.

Compromise: the unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other CSPs).

Confidentiality: the property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

Critical security parameter (CSP): security-related information (e.g., secret and private cryptographic keys, authentication data such as passwords and PINs) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a CIMC or the security of the information protected by the CIMC.

Cryptographic key (key): a parameter used in conjunction with a cryptographic algorithm that determines:

- the transformation of plaintext data into ciphertext data,
- the transformation of ciphertext data into plaintext data,
- a digital signature computed from data,
- a keyed hash computed from data,
- the verification of a digital signature computed from data,
- an authentication code computed from data, or
- an exchange agreement of a shared secret.

Cryptographic key component (key component): a parameter used in conjunction with other key components in a FIPS-approved or recommended security method to form a plaintext cryptographic key or perform a cryptographic function.

Digital signature: a non-forgeable transformation of data that allows proof of the source (with non-repudiation) and verification of the integrity of that data.

Encrypted key: a cryptographic key that has been encrypted with a key encrypting key, a PIN or a password in order to disguise the value of the underlying plaintext key.

Error detection code (EDC): a code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.

FIPS-Approved or recommended mode of operation: a mode that employs only the operation of FIPS-approved or recommended security methods.

FIPS-approved or recommended security method: a security method (e.g., cryptographic algorithm, cryptographic key generation algorithm or key distribution technique, authentication technique, or

[4] The terms in this standard are based on terms defined in FIPS PUBs. The terms have been tailored for a CIMS.

evaluation criteria) that is either a) specified in a FIPS or b) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.

Firmware: the programs and data stored in hardware (e.g., ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution.

Hardware: the physical equipment used to process programs and data in a CIMC.

Integrity: the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Key encrypting key: a cryptographic key that is used for the encryption or decryption of other keys.

Key management: the activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs, passwords) during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving.

Password: a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Personal Identification Number (PIN): a 4 or more character alphanumeric code or password used to authenticate an identity, commonly used in banking applications.

Physical protection: the safeguarding of a CIMC, cryptographic keys, or other CSPs using physical means.

Plaintext key: an unencrypted cryptographic key.

Private key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public.

Protection Profile: an implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs.

Public key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public. (Public keys are not considered CSPs.)

Public key certificate: a set of data that unambiguously identifies an entity, contains the entity's public key, is digitally signed by a trusted party, and binds the public key to the entity.

Public key (asymmetric) cryptographic algorithm: a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that, given the public key, it is computationally infeasible to derive the private key.

Secret key: a cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and which shall not be made public. The use of the term "secret" in this context does not imply a classification level rather the term implies the need to protect the key from disclosure or substitution.

Secret key (symmetric) cryptographic algorithm: a cryptographic algorithm that uses a single, secret key for both encryption and decryption.

Security policy: a precise specification of the security rules under which a CIMC shall operate, including the rules derived from the requirements of this document and additional rules imposed by the vendor.

Software: the programs and associated data that can be dynamically written and modified.

Split knowledge: a condition under which two or more entities separately have key components that individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module.

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF) - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

Trusted path: a means by which an operator and a TSF can communicate with the necessary confidence to support the TSP.

User: an individual, or a process (subject) operating on behalf of the individual, accessing CIMC.

Zeroization: a method of erasing electronically stored data by altering or deleting the contents of the data storage so as to prevent the recovery of the data.

11 ACRONYMS

ANSI	American National Standards Institute
CA	Certification Authority
CC	Evaluation Criteria for Information Technology Security (Common Criteria)
CIMC	Certificate Issuing and Management Component
CIMS	Certificate Issuing and Management System
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration Authority
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy